Opinia prawna

Konflikt interesów w wykonywaniu funkcji inspektora ochrona danych i jego unikanie. Problemy zaistniałe w praktyce i sposoby ich rozwiązania.

autor: dr hab. Grzegorz Sibiga, prof. INP PAN

Opinia przygotowana na zlecenie: SABI Stowarzyszenia Inspektorów Ochrony Danych oraz Związku Firm Ochrony Danych Osobowych.

SABI Stowarzyszenie Inspektorów Ochrony Danych

ZFODO

Warszawa, dnia 5 kwietnia 2024 r.

Spis treści

1. Przedmiot opinii ... 5

Stanowisko autora opinii – synteza ... 6

2. Analiza prawna ... 7

Część I. Konflikt interesów – rozumienie pojęcia i cele unikania tego konfliktu ... 7

„Konflikt interesów" w znaczeniu słownikowym ... *8*

„Konflikt interesów" w ujęciu nauk prawnych i innych nauk społecznych ... *9*

Konflikt interesów w działalności regulowanej w prawie ... *10*

Radca prawny ... *10*

Adwokat ... *10*

Doradca podatkowy ... *11*

Konflikt interesów w zasadach etyki księgowych ... *11*

Podsumowanie ... 13

Część II. Zasady wykonywania funkcji inspektora ochrony danych (IOD) określone w art. 38 ust. 6 RODO i cele ich wprowadzenia ... 13

Rodzaje konfliktów interesów w ochronie danych osobowych ... 17

Konflikt interesów o charakterze ustrojowym ... 18

Konflikt interesów o charakterze merytorycznym ... 18

Decydowanie o celach i sposobach przetwarzania danych osobowych ... *18*

Pełnienie funkcji IOD w dwóch podmiotach o sprzecznych interesach ... *19*

Konflikt interesów o charakterze czasowym ... 20

Unikanie konfliktu interesów w działalności IOD ... 21

Część III. Dodatkowe zadania i obowiązki IOD ... 23

Udział IOD w tworzeniu dokumentacji przetwarzania danych osobowych ... 24

Prowadzenie przez IOD RCP oraz RCKP ... 25

Dokumentowanie przez IOD naruszeń zgodnie z art. 33 ust. 5 RODO ... 31

Udział IOD w ocenie skutków dla ochrony danych osobowych ... 32

Udział IOD w tworzeniu dokumentów wewnętrznych dotyczących ochrony danych osobowych w organizacji ... 33

Pełnienie roli pełnomocnika administratora (podmiotu przetwarzającego) ... 35

Kierowanie pracami zespołu IOD oraz korzystanie z zasobów administratora ... 37

Część IV. Wpływ formy wykonywania funkcji IOD (wewnętrzny oraz outsourcing) na konflikt interesów oraz jego unikanie ... 38

Outsourcing funkcji IOD ... 38

Pełnienie funkcji IOD jako członek personelu administratora (podmiotu przetwarzającego) ... 40

V. Możliwe modele pełnienia funkcji IOD ... 42

Model statyczny ... 44

Model dynamiczny ... 45

3. Wnioski ... 47

Załącznik nr 1 - Wykaz źródeł ... 50

Załącznik nr 2 - Stanowiska organu ochrony danych osobowych dotyczące konfliktu interesów IOD ... 54

Wykaz użytych skrótów

DPIA – ocena skutków dla ochrony danych osobowych w rozumieniu art. 35 ust. 1 RODO

Dyrektywa 95/46/WE - Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

EROD – Europejska Rada Ochrony Danych

IOD – Inspektor Ochrony Danych w rozumieniu art. 37 RODO

KEA - Zbiór Zasad Etyki Adwokackiej i Godności Zawodu (Kodeks Etyki Adwokackiej)

KERP - Kodeks Etyki Radcy Prawnego stanowiący załącznik do uchwały nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014 r. uwzględniający zmiany wprowadzone uchwałą Nr 1/2022 Krajowego Zjazdu Radców Prawnych z dnia 8 lipca 2022 r. w sprawie zmiany Kodeksu Etyki Radcy Prawnego

KPA – ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. 2023 poz. 775 ze zm.)

PPSA – ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. 2023 poz. 1634 ze zm.)

Raport EROD – raport Europejskiej Rady Ochrony Danych przyjęty 16 stycznia 2024 r. w ramach skoordynowanego działania egzekwowania prawa (CEF) w 2023 r., dotyczącego wyznaczenia i pozycji inspektorów ochrony danych

RCKP - rejestr kategorii czynności przetwarzania dokonywanych art. 30 ust. 2 RODO

RCP – rejestr czynności przetwarzania danych osobowych w rozumieniu art. 30 ust. 1 RODO

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L. z 2016 r. nr 119, str. 1, z późn. zm.);

rozporządzenie 2018/1725 – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. U. UE. L. z 2018 r. Nr 295, str. 39).

TSUE - Trybunał Sprawiedliwości Unii Europejskiej

UDP - ustawa z dnia 5 lipca 1996 r. o doradztwie podatkowym (t.j. Dz. U. z 2021 r. poz. 2117)

URP - ustawa z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2022 r. poz. 1166 z późn. zm.)

Ustawa z 1997 r. – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 poz. 922)

Ustawa z 2018 r. – ustawa z 10 maja 20218 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781 ze zm.)

Wytyczne (243) - Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych, WP 243 rew. 01

Wytyczne (250) – Wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250)

Wytyczne 09/2022 - Wytyczne EROD z 28 marca 2023 nr 09/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych zgodnie z RODO

ZEDP - Załącznik do uchwały nr 12/2022 Krajowej Rady Doradców Podatkowych z dnia 14 lutego 2022 r. w sprawie przyjęcia tekstu jednolitego Zasad etyki doradców podatkowych - Zasady Etyki Doradców Podatkowych

1. Przedmiot opinii

1. Przedmiotem niniejszej opinii jest ustalenie istoty konfliktu interesów, który może występować w wykonywaniu funkcji inspektora ochrony danych.
2. W pierwszej części analizy prawnej opinii zostanie wyjaśnione:
    1) znaczenie pojęcia konfliktu interesów na gruncie przepisów wymagających jego unikania przez przedstawicieli grupy osób zajmujących określone stanowiska lub wykonujące określony zawód (analiza nie obejmuje jednocześnie sytuacji, w których konflikt interesów i jego unikanie jest jedynie postulatem, a nie wymogiem wykonywania zawodu bądź zajmowania stanowiska);
    2) zasadność statuowania obowiązku unikania konfliktu interesów w przypadku wykonywania określonego zawodu lub zajmowania stanowiska.
3. W drugiej części analizy prawnej opinii – z uwzględnieniem ustaleń poczynionych w pierwszej części opinii - zostaną omówione:
    1) rozumienie konfliktu interesów w ochronie danych osobowych oraz rodzaje tych konfliktów w działalności IOD,
    2) konflikt interesów o charakterze ustrojowym,
    3) konflikt interesów o charakterze merytorycznym,
    4) konflikt interesów o charakterze czasowym,
    5) unikanie konfliktu interesów w działalności IOD.
4. W trzeciej części przeanalizowano potencjalne dodatkowe zadania i obowiązki realizowane przez IOD z obszaru ochrony danych osobowych, w kontekście występowania konfliktu interesów, w tym:
    1) udział IOD w tworzeniu dokumentacji przetwarzania danych osobowych,
    2) prowadzenie przez IOD RCP oraz RCKP,
    3) dokumentowanie przez IOD naruszeń zgodnie z art. 33 ust. 5 RODO,
    4) udział IOD w ocenie skutków dla ochrony danych osobowych,
    5) udział IOD w tworzeniu dokumentów wewnętrznych dotyczących ochrony danych osobowych w organizacji,
    6) pełnienie roli pełnomocnika administratora (podmiotu przetwarzającego),
    7) kierowanie pracami zespołu IOD oraz korzystanie z zasobów administratora.
5. W kolejnej części wskazano wpływ formy wykonywania funkcji IOD na konflikt interesów i jego unikanie poprzez omówienie:
    1) outsourcingu funkcji IOD,
    2) pełnienia funkcji IOD jako członek personelu administratora (podmiotu przetwarzającego),
    3) wpływ formy wykonywania funkcji IOD (wewnętrzny oraz outsourcing) na konflikt interesów oraz jego unikanie
    4) unikanie konfliktu interesów w działalności IOD i postępowanie z tym związane.

6. W ostatnich częściach opinii przedstawiono wnioski, w tym zaproponowano modele wykonywania funkcji IOD.

Stanowisko autora opinii – synteza

1. Celem unikania konfliktu interesów jest zapewnienie prawidłowości wykonywanego zawodu lub funkcji. Konsekwencją konfliktu interesów jest brak niezależności i obiektywizmu w pełnieniu funkcji oraz wykonywanie jednocześnie zadań na zlecenie podmiotów, które mają lub mogą mieć sprzeczne ze sobą interesy w danym obszarze.
2. Pojęcie „konflikt interesów" oznacza istnienie kolidującego z interesem polegającym ma prawidłowym realizowaniu zadania (np. wykonywanie zawodu czy funkcji) innego interesu (lub interesów) tej samej osoby, czyli taki (takie), które uniemożliwiają prawidłowe działanie.
3. Pod pojęciem „prawidłowe działania" (prawidłowego wykonywania zadania) rozumiem działanie według przyjętego w prawie lub zasadach etycznych wzorca postępowania. Takim wzorem może być postępowanie niezależne, bezstronne, obiektywne, bezinteresowne lub lojalne wobec klienta. Interesy kolidujące z tym wzorcem są związane z sytuacją osobistą wykonującego zadania (jego własną lub dotyczącą osób najbliższych) lub innymi wartościami (interesami), które realizuje ta osoba (np. nakierowanie na inne cele niż wymienione powyżej, choćby lojalność wobec innych podmiotów).
4. Konflikt interesów w wykonywaniu funkcji IOD o którym mowa w art. 38 ust. 6 RODO ma charakter częściowo autonomiczny. Konflikt ten występuje w sytuacji, jeżeli inne nałożone na IOD zadania i obowiązki uniemożliwiają prawidłowe wykonywanie zadań IOD określonych w art. 39 RODO.
5. Przez prawidłowe wykonywanie zadań IOD rozumiem ich realizowanie w sposób niezależny, obiektywny oraz skuteczny.
6. Występowanie konfliktu interesów w wykonywaniu funkcji IOD ma charakter obiektywny i jest uzależniony od okoliczności faktycznych, które muszą zostać wzięte pod uwagę przy ocenie, czy sposób oraz warunki wykonywania zadań IOD będą prowadzić do rzeczywistego konfliktu interesów.
7. Zasadą jest, że IOD może wykonywać dodatkowe zadania i obowiązki nałożone przez administratora (podmiot przetwarzający). Wyjątkową sytuacją jest natomiast występowanie konfliktu interesów, który będzie uniemożliwiał wykonywanie jednocześnie dodatkowych zadań i prawidłowe sprawowanie funkcji IOD. Kwalifikację sytuacji powodującej konflikt interesów na gruncie przepisów o ochronie danych osobowych należy przeprowadzać ostrożnie i wąsko.
8. W obszarze ochrony danych osobowych administrator (podmiot przetwarzający) przy nakładaniu dodatkowych zadań może wziąć pod uwagę to, że głównym celem istnienia i aktywności IOD jest jego wsparcie - w dopuszczalnym zakresie - w realizacji obowiązków ustalonych w RODO, w szczególności zważywszy na kwalifikacje zawodowe IOD, które są podstawą jego wyznaczenia. Granicą tych dodatkowych zadań jest naruszenie nimi niezależności, obiektywizmu i skuteczności działań IOD.

9. W ocenie autora niniejszej opinii możliwe jest wykonywanie funkcji IOD w dwóch modelach, tj. statycznej i dynamicznej:
    a. **Model statyczny** zakłada, że rolą IOD w organizacji jest przede wszystkim monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz zasad przyjętych w organizacji i sygnalizowanie nieprawidłowości, jednak bez wskazywania konkretnych rozwiązań dostrzeżonych uchybień (np. projektu prawidłowego dokumentu wewnętrznego). Rolą IOD jest również podnoszenie świadomości w obszarze ochrony danych osobowych w organizacji. Doradzanie, będące jednym z zadań IOD sprowadza się do podnoszenia świadomości samego administratora (podmiotu przetwarzającego) jak i jego personelu, w obszarze ochrony danych osobowych. W tym modelu IOD w praktyce ogranicza swoją działalność wyłącznie do wąsko rozumianych zadań wskazanych w art. 39 ust. 1 RODO;
    b. **Model dynamiczny** zakłada, że IOD nie tylko monitoruje przestrzeganie przepisów o ochronie danych osobowych oraz zasad przyjętych w organizacji i sygnalizuje nieprawidłowości, ale też bierze aktywny udział w rozwiązaniu stwierdzonych uchybień, poprzez przedstawienie konkretnych możliwych rozwiązań administratorowi, choć co ważne, nie decyduje o ich ostatecznym kształcie i nie wdraża ich. IOD wykonuje przy tym zwykle dodatkowe zadania związane z ochroną danych osobowych w organizacji, obowiązki dokumentacyjne, takie jak prowadzenie RCP, RCKP, dokumentuje naruszenia, projektuje treść obowiązków informacyjnych dla podmiotów danych.
10. W ocenie autora oba modele są możliwe do zastosowania przez administratora lub podmiot przetwarzający w swojej organizacji.

2. Analiza prawna

Część I. Konflikt interesów – rozumienie pojęcia i cele unikania tego konfliktu

Punktem wyjścia do dalszej analizy jest ustalenie znaczenia pojęcia „konflikt interesów". W tym celu należy odnieść się do językowego znaczenia tego pojęcia w języku polskim oraz w językach obcych, a także do jego rozumienia w naukach prawnych i innych naukach społecznych. Istotne znaczenie będzie miało również przedstawienie znaczenia „konfliktu interesów" w przypadku osób wykonujących zawody (funkcje), w których działalności reguluje się istnienie konfliktu interesów i jego unikanie.

Nieodłącznie związane z konfliktem interesów jest „unikanie konfliktu interesów", który to zwrot również wymaga wyjaśnienia. Z założenia konflikt interesów jest sytuacją niepożądaną, w tym znaczeniu, że trzeba mu zapobiec, a gdy już do niego dojdzie doprowadzić do sytuacji, gdy nie będzie on już występował.

Co istotne, wyjaśniane zwroty („konflikt interesów", „unikanie konfliktu interesów") występują zawsze kontekście prawidłowej realizacji celów określonej działalności konkretnych podmiotów lub osób. Konflikt interesów uniemożliwia bowiem taką prawidłową realizacją celów aktywności osób i podmiotów. Dlatego wyjaśniając naturę konfliktu interesów należy równocześnie wyjaśnić cele zajmowania się tym zjawiskiem, w szczególności, dlaczego musimy mu przeciwdziałać.

„Konflikt interesów" w znaczeniu słownikowym

Zwrot „konflikt interesów" składa się z dwóch wyrazów „konflikt" oraz „interes". Zgodnie z ich gramatycznym znaczeniem w języku polskim pojęcia te należy rozumieć w następujący sposób:

- **Konflikt** (łać. *conflictus*) to m.in. zdarzenie, sprzeczność interesów, poglądów, spór, antagonizm przedłużająca się niezgoda pomiędzy stronami lub różnica pomiędzy wartościami, postawami itp., której nie sposób usunąć[1]. Jest to wszelkie zetknięcie się sprzecznych dążeń[2].
- **Interes (**łać. *interesse)* to m.in. jako branie w czymś udziału, sprawy obchodzące kogoś, rzecz ważna, jako sprawa do załatwienia, pożytek, korzyść lub przedsięwzięcie przynoszące korzyść materialną[3]. "Interes" można interpretować także jako "przedmioty lub stan rzeczy, których osiągnięcie jednostki lub grupy społeczne uważają za pożądane lub konieczne i dla osiągnięcia, których mobilizują swą aktywność i środki[4].

Łącząc zwykłe znaczenia nadawane w języku polskim wyrazom „konflikt", „interes" oraz zwrotowi „konflikt interesów", sformułowanie to literalnie można rozumieć jako istnienie dwóch kolidujących ze sobą (niezgodnych) interesów (spraw do załatwienia, przedsięwzięć) w określonym stanie faktycznym, które nie pozwalają podjąć uczciwej decyzji.

Podobne znaczenie przypisuje się „konfliktowi interesu" w innych językach. W słowniku języka angielskiego wydawnictwa Cambridge konflikt interesów (ang. *conflict of interests*) określono jako sytuację, w której dana osoba nie może podejmować sprawiedliwej, uczciwej decyzji, ponieważ skutki decyzji będą miały na nią wpływ[5]. W słowniku wydawnictwa Longman „konflikt interesów" przedstawia się jako sytuację, w której dana osoba nie może wykonywać swojej pracy uczciwie, ponieważ ma moc decydowania o czymś w sposób, który byłby dla niej korzystny, chociaż może to nie być najlepsza decyzja[6]. W słowniku języka angielskiego wydawnictwa Merriam-Webster wskazuje się, że konflikt interesów może oznaczać:

- konflikt między prywatnymi interesami a służbowymi lub zawodowymi obowiązkami osoby zajmującej stanowisko wymagające zaufania,

[1] Słownik języka polskiego PWN, w opracowaniu E. Sobol i innych, Wydawnictwo Naukowe PWN, Warszawa 2011, str. 346; Uniwersalny słownik języka polskiego, red. S. Dubisz, Wydawnictwo Naukowe PWN, Warszawa 2008, tom K-Ó, str. 202; Słownik języka polskiego PWN, red. M. Szymczak, Wydawnictwo Naukowe PWN Warszawa 1996, tom I A-K, str. 925.; J. Sondel, Słownik łacińsko-polski, Kraków 2009.

[2] Encyklopedia powszechna PWN, t. II, Warszawa 1984, s. 541.

[3] Słownik Języka Polskiego, Definicja pojęcia „interes" dostępna pod adresem: https://sjp.pwn.pl/sjp/interes;2466578.html; Wielka Encyklopedia PWN, red. J. Wojnowski, t. XII, Warszawa 2002, s. 186., J. Pieńkos, Słownik łacińsko-polski. Łacina w nauce i kulturze, Warszawa 1996, s. 216.; J. Sondel, Słownik łacińsko-polski, Kraków 2009 s. 512.

[4] Nowy Leksykon PWN, red. A. Dyczkowski, Warszawa 1998, s. 684.

[5]Cambridge Dictionary, definicja pojęcia „conflict of interests" dostępna pod adresem URL : https://dictionary.cambridge.org/dictionary/english-polish/conflict?q=conflict+of+interest#google_vignette, dostęp: 5.04.2024 r.).

[6] Longman Business Dictionary, Conflict of ˈinterest noun (plural conflicts of interest) [countable, uncountable] a situation in which you cannot do your job fairly because you have the power to decide something in a way that would be to your advantage, although this may not be the best decision – definicja dostępna pod adresem URL: https://www.ldoceonline.com/dictionary/conflict-of-interest (dostęp: 5.04.2024 r.).

- konflikt między konkurującymi obowiązkami (np. reprezentowanie przez adwokata klientów o przeciwnych interesach)[7].

Z kolei w języku niemieckim „konflikt interesów" (*der Interessenkonflikt*) jest definiowany jako „sprzeczność wynikającą z rozbieżnych interesów"[8].

„Konflikt interesów" w ujęciu nauk prawnych i innych nauk społecznych

W języku prawniczym pod pojęciem „interesu" rozumie się jako "ujawnioną w określonej strukturze społecznej i uświadomioną potrzebę, wychodząc z założenia, że u podstaw określonych, świadomych zachowań jednostek bądź grup społecznych leżą zawsze jakieś uświadomione potrzeby tych podmiotów" [9]. Konflikt jest natomiast postrzegany jako „układ wzajemnych wartości (potrzeb) w którym wartości te wykluczają się bądź też realizacja jednych utrudnia realizację innych"[10]. Konflikt interesów można zatem rozumieć jako skierowane przeciwko sobie działania co najmniej dwóch podmiotów, które dążą do realizacji własnych interesów (potrzeb) i napotykających przeciwdziałanie innych zainteresowanych osób dążących do realizacji swoich interesów[11].

Podobne ujęcie „konfliktów interesu" występuje w naukach socjologicznych, w których wskazuje się, że jest sytuacja, gdy własny interes uniemożliwia danej osobie wykonywanie obowiązków zawodowych lub publicznych w sposób obiektywy (bezstronny), co powoduje m.in. zmniejszenie skuteczności takiej osoby w wykonywaniu jej zawodowych obowiązków[12]. Podkreśla się przy tym, że konflikt interesów ma miejsce, gdy zakres interesów danej osoby ma potencjał do kolidowania z prawidłowym dokonywaniem przez nią osądu spraw innej osoby[13].

W naukach psychologicznych konflikt interesów postrzega się m.in. jako zespół okoliczności, które stwarzają ryzyko, że na profesjonalny osąd lub działania dotyczące interesu pierwotnego nadmierny wpływ będzie miał interes wtórny[14]. W ocenie badaczy do konfliktu dochodzi w przypadku sprzeczności lub niezgodności interesów w ważnej dla danych osób, grup sprawie, gdy takie osoby wejdą ze sobą w interakcję i będą się postrzegać jako osoby zamierzające sobie wzajemnie zaszkodzić[15].

---

[7] Merriam-Webster.com Dictionary, Merriam-Webster, Conflict of interest: (1) a conflict between the private interests and the official or professional responsibilities of a person in a position of trust, (2) a conflict between competing duties (as in an attorney's representation of clients with adverse interests) - definicja dostępna pod adresem URL: https://www.merriam-webster.com/dictionary/conflict%20of%20interest (dostęp: 5.04.2024 r.).

[8] Słownik wydawnictwa Duden, Interessenkonflikt – definicja dostępna pod adresem URL: https://www.duden.de/rechtschreibung/Interessenkonflikt (dostęp: 5.04.2024 r.).

[9] M.Myślińska, A. Szot, Analiza konfliktowa w administracyjnym typie stosowania prawa (zarys problematyki), [w:] red. M. Chrzanowski, J. Kostrubiec, I. Nowikowski, red., Państwo, prawo, polityka. Księga poświęcona pamięci Profesora Henryka Groszyka, Lublin 2012, s. 231

[10] M. Wyrzykowski, Pojęcie interesu społecznego w prawie administracyjnym, Warszawa 1986, s. 164.

[11] M. Myślińska, A. Szot, Analiza konfliktowa w administracyjnym typie..., s. 231 i przywołana tam literatura.

[12] American Sociological Association, Topic: Conflicts of Interest, https://www.asanet.org/topic-conflicts-of-interest/ (dostęp: 5.04.2024 r.).

[13] M. Davis, Conflict of Interest [w:] R. Chadwick, red., Encyclopedia of Applied Ethics (Second Edition), Academic Press, 2012, Pages 571-577.

[14] E. B. Rubin, Chapter 7 - Professional conduct and misconduct, [w:] J. L. Bernat, H. R. Beresford, red., Handbook of Clinical Neurology, 2013, s. 91-105.

[15] H. Hamer, Psychologia społeczna. Teoria i praktyka, Warszawa 2005, s. 270.

Biorąc powyższe pod uwagę, można uznać, że w naukach prawnych oraz w innych naukach społecznych pojęcie konfliktu interesu jest zatem rozumiane jako kolizja wartości, która negatywnie wpływa na prawidłowość wykonywania zadań przez jednostkę na rzecz innej osoby.

Konflikt interesów w działalności regulowanej w prawie

Radca prawny

Obowiązek unikania konfliktu interesów występuje w wielu obszarach prawach. W szczególności obowiązek unikania konfliktu interesów dotyczy osób wykonujących zawody zaufania publicznego, który wynika z poszczególnych ustaw jak i kodeksów etycznych dla poszczególnych zawodów.

W przypadku radcy prawnego zgodnie z art. 15 URP jest on obowiązany wyłączyć się od wykonania czynności zawodowych we własnej sprawie lub jeżeli przeciwnikiem jednostki organizacyjnej udzielającej mu pełnomocnictwa jest inna zatrudniająca go jednostka organizacyjna lub jeżeli sprawa dotyczy osoby, z którą pozostaje on w takim stosunku, że może to oddziaływać na wynik sprawy. W doktrynie wskazuje się, że konflikt interesów przy wykonywaniu zawodu radcy prawnego ma miejsce, gdy radca prawny działa w interesie dwóch lub większej liczby klientów w zakresie tych samych lub powiązanych ze sobą spraw, a wykonywanie przez niego zadania na rzecz klientów "stoją ze sobą w sprzeczności lub istnieje ryzyko, iż mogłyby one stać ze sobą w sprzeczności."[16] .

W art. 10 ust. 1 KERP doprecyzowano cel wprowadzenia obowiązku unikania konfliktu interesów. Służy on zapewnieniu **niezależności, dochowaniu tajemnicy zawodowej oraz lojalności wobec klienta.** Sytuacje, w których występuje konflikt interesów w pracy radcy prawnego zostały określone w art. 26-30 KERP. Jak wskazuje doktryna niezależność, tajemnica zawodowa oraz lojalność wobec klienta to konstytutywne cechy zawodu radcy prawnego, bez których nie mógłby on być wykonywany[17]. Z tego wynika, że uniknięcie konfliktu interesów ma celu zapewnienie jego niezależności, zachowania w tajemnicy informacji pozyskanych od klienta oraz zapewnienie lojalności.

W art. 26 ust. 1 KERP określono, że taki konflikt interesów występuje, gdy dochodzi do naruszenia lub zagrożenia naruszenia tajemnicy zawodowej, ograniczenia **lub stworzenia zagrożenie naruszenia niezależności** lub gdy wiedza o sprawach innego klienta, na którego rzecz wcześniej wykonywał czynności zawodowe dawałoby klientowi nieuzasadnioną przewagę (art. 26 KERP). W tych sytuacjach radca prawny powinien powstrzymać się od czynności zawodowych, aby uniknąć konfliktu interesów.

Adwokat

Z § 22 KEA wynika zakaz działania przez adwokata w stanie konfliktu interesów. Sam konflikt interesów został sformułowany w sposób opisowy i dotyczy takich sytuacji jak: udzielenie wcześniej pomocy prawnej stronie przeciwnej w tej samej sprawie lub w sprawie z nią związanej; udział w tej sprawie, wykonując funkcję publiczną; osoba, przeciwko której adwokat ma prowadzić sprawę, jest jego klientem, choćby w innej sprawie oraz jeżeli zawodowy

[16] K. Kwapisz, Ustawa o radcach prawnych. Komentarz, Warszawa 2011, art. 15.
[17] T. Scheffler (red.), Kodeks Etyki Radcy Prawnego. Komentarz. Wyd. 4, Warszawa 2023.

pełnomocnik będący dla niego osobą najbliższą prowadzi sprawę lub udzielił już pomocy prawnej stronie przeciwnej w tej samej sprawie lub w sprawie z nią związanej.

Jak wskazuje się w doktrynie działanie adwokata w sytuacji, gdy występuje konflikt interesów może naruszać jego podstawowe obowiązki etyczne:

- obowiązek lojalności wobec klienta;
- obowiązek dochowania tajemnicy adwokackiej i dyskrecji;
- obowiązek przedstawienia klientowi wszystkich informacji (w granicach posiadanej wiedzy), które są istotne z punktu widzenia prowadzenia sprawy w interesie klienta;
- obowiązek nieprzedkładania interesu własnego lub osób trzecich ponad interes klienta[18].

W związku z powyższym unikanie konfliktu interesów ma na celu wykonywanie w prawidłowy sposób przez adwokata jego obowiązków etycznych.

Doradca podatkowy

Wykonywanie zawodu doradcy podatkowego wiąże się również z koniecznością unikania konfliktu interesów. Konflikt interesów doradcy podatkowego może mieć co najmniej trzy wymiary.

Pierwszy wymiar to wykonywanie przez doradcę podatkowego innego rodzaju działalności gospodarczej lub pozostawanie w stosunku zatrudnienia. Zgodnie z art. 31 ust. 1 UDP:

> 1. Doradca podatkowy wykonujący ten zawód może prowadzić działalność gospodarczą lub być zatrudniony, jeżeli jej wykonywanie lub to zatrudnienie:
>
> 1) nie powoduje konfliktu interesów i niezgodności między poszczególnymi rodzajami działalności lub zatrudnienia;
>
> 2) nie narusza niezależności i bezstronności doradcy podatkowego;
>
> 3) nie pozostaje w sprzeczności z zasadami etyki zawodowej doradcy podatkowego.

Drugi wymiar to konflikt interesów pomiędzy doradcą podatkowym, a jego klientem, którego sprawy wcześniej rozstrzygał, zgodnie z art. 32 ust. 1 UDP:

> „Doradca podatkowy, w ciągu 2 lat od dnia wpisu na listę, nie może wykonywać doradztwa podatkowego na rzecz osób, których sprawy rozstrzygał w ciągu ostatnich 3 lat przed ustaniem zatrudnienia lub pełnienia funkcji."

W art. 10 ust. 1 ZEDP określono również sytuacje, w których występuje konflikt interesów w związku z reprezentowaniem stron transakcji o przeciwstawnych interesach lub gdy sytuacja procesowa stron powoduje, że sukces jednej strony oznacza porażkę drugiej strony. W art. 10 ust. 4 ZEDP nałożono na doradcę podatkowego obowiązek podjęcia kroków zmierzających do eliminacji konfliktu interesów lub zaprzestania świadczenia usług powodujących konflikt.

Konflikt interesów w zasadach etyki księgowych

[18] J. Naumann, Zbiór Zasad Etyki Adwokackiej i Godności Zawodu. Komentarz. Wyd. 5, Warszawa 2023, §22.

W Podręczniku Międzynarodowego kodeksu etyki zawodowych księgowych w tym Międzynarodowych standardów niezależności określono szczegółowo zasady występowania i unikania konfliktu interesów[19]. Podręcznik ten stanowi m.in. Załącznik do uchwały Nr 207/7a/2023 Krajowej Rady Biegłych Rewidentów z dnia 17 grudnia 2023 r. w sprawie ustanowienia zasad etyki zawodowej biegłych rewidentów.

Zasady dotyczące konfliktu interesów zostały sformułowane odrębnie dla sytuacji, gdy:

- zawodowy księgowy jest zatrudniony w przedsiębiorstwach (Część 2) oraz
- zawodowy księgowy wykonuje wolny zawód (Część 3).

Zgodnie z pkt 210.2 ww. Zasad „Konflikt interesów **stwarza zagrożenia dla przestrzegania zasady obiektywizmu** i może stworzyć zagrożenia dla przestrzegania innych podstawowych zasad". Takie zagrożenia mogą powstać, gdy zawodowy księgowy podejmuje się wykonania czynności zawodowej związanej z określoną sprawą dla dwóch lub większej liczby stron, których interesy dotyczące tej sprawy są sprzeczne; lub interes zawodowego księgowego dotyczący określonej sprawy i interesy strony, dla której księgowy podejmuje się wykonania czynności zawodowej odnoszącej się do tej sprawy, są sprzeczne.

Po stronie zawodowego księgowego ciąży obowiązek identyfikacji konfliktów interesów i związanych z nimi zagrożeń (pkt R210.5). Przykładem czynności, która może wyeliminować zagrożenia spowodowane przez konflikty interesów, jest wycofanie się z procesu podejmowania decyzji odnoszącego się do sprawy, która stanowi źródło konfliktu interesów (pkt 210.7 A2). Jako przykład działań, które mogą stanowić zabezpieczenie w reakcji na zagrożenia spowodowane przez konflikty interesów, należy wskazać reorganizację lub podział określonych odpowiedzialności i obowiązków (pkt 210.7 A3).

Podobnie w przypadku zawodowego księgowego wykonującego wolny zawód zgodnie z pkt 310.2 „Konflikt interesów stwarza zagrożenia dla przestrzegania zasady obiektywizmu i może wywołać zagrożenia dla przestrzegania innych podstawowych zasad. Takie zagrożenia mogą powstać, gdy: (a) zawodowy księgowy świadczył usługę profesjonalną związaną z określoną sprawą dla dwóch lub większej liczby klientów, których interesy dotyczące tej sprawy są sprzeczne; lub (b) interesy zawodowego księgowego dotyczące określonej sprawy i interesy klienta, dla którego zawodowy księgowy świadczy usługę profesjonalną odnoszącą się do tej sprawy, są sprzeczne".

Zgodnie z pkt. R310.5 „Przed akceptacją współpracy z nowym klientem, zlecenia lub współpracy gospodarczej zawodowy księgowy podejmuje odpowiednie działania w celu zidentyfikowania okoliczności, które mogłyby powodować konflikt interesów i związane z nim zagrożenie dla przestrzegania jednej lub większej liczby podstawowych zasad. Takie działania obejmują identyfikację: (a) rodzaju istotnych interesów, udziałów (ang. interests) i powiązań pomiędzy zaangażowanymi stronami; oraz (b) usługi i jej skutków dla zaangażowanych stron".

W tym przypadku jako działania mające na celu zabezpieczenie w reakcji na zagrożenia wywołane przez konflikt interesów, obejmują posiadanie odrębnych zespołów wykonujących zlecenie, którym przekazano jasne polityki i procedury co do zachowania poufności lub zaangażowanie odpowiedniego kontrolera, który nie jest zaangażowany w świadczenie danej

[19]Dokument dostępny pod adresem URL: https://www.pibr.org.pl/assets/meta/7793,207_za%C5%82.%20do%20uchwa%C5%82y_Kodeks%20IESBA%202022_fin.pdf (dostęp: 5.04.2024 r.).

usługi i na którego dany konflikt nie wpływa w inny sposób, do przeprowadzenia przeglądu pracy w celu oceny, czy kluczowe osądy i wnioski są odpowiednie (pkt 310.8 A3).

Ponadto zarówno dla księgowych zawodowych w przedsiębiorstwach jak i dla wykonujących wolny zawód jako zagrożenie dla wykonywania zawodu jest wskazana **autokontrola,** które może polegać, w szczególności, na:

- niewłaściwej ocenie wyników wcześniej dokonanego osądu lub czynności wykonanej przez księgowego lub inną osobę w firmie księgowego lub organizacji zatrudniającej księgowego, na których księgowy będzie polegał przy formułowaniu osądu w ramach wykonywania bieżącej czynności (pkt 120.6 A3 (b));
- wydaniu przez zawodowego księgowego raportu atestacyjnego na temat skuteczności funkcjonowania wdrożonych przez niego systemów finansowych (pkt 300.6 A1 (b));
- przygotowaniu przez zawodowego księgowego źródłowych danych wykorzystanych do sporządzania zapisów, które stanowią zagadnienie będące przedmiotem zlecenia atestacyjnego (pkt 300.6 A1 (b)).

Mając na uwadze powyższe należy zatem uznać, że konflikt interesów w przypadku działalności regulowanej oznaczać będzie sytuacje, w którym osoba wykonująca dany zawód ze względu na sprzeczne obowiązki nie jest w stanie dokonywać swoich powierzonych jej zadań przez klienta w **obiektywy i lojalny sposób**.

Podsumowanie

Podsumowując część wprowadzającą opinii przyjmuję, że „konflikt interesów" oznacza istnienie kolidującego z interesem polegającym ma prawidłowym realizowaniu zadania (np. wykonywanie zawodu czy funkcji) innego interesu (lub interesów) tej samej osoby, czyli taki (takie), które uniemożliwiają prawidłowe działanie. Pod pojęciem „prawidłowe działania" (prawidłowego wykonywani zadania) rozumiem działanie według przyjętego w prawie lub zasadach etycznych wzorca postępowania. Takim wzorem może być postępowanie niezależne, bezstronne, obiektywne, bezinteresowne lub lojalne wobec klienta. Interesy kolidujące z tym wzorcem są związane z sytuacją osobistą wykonującego zadania (jego własną lub dotyczącą osób najbliższych) lub innymi wartościami (interesami), które realizuje ta osoba (np. nakierowanie na inne cele niż wymienione powyżej, choćby lojalność wobec innych podmiotów).

Inaczej ujmując, określona osoba lub podmiot nie mogą wykonywać zadania prawidłowo (tj. niezależne, bezstronne, obiektywne, bezinteresowne, lojalnie) ponieważ zaistniała sytuacja jego dotycząca lub występują wartości odnoszące się do niego, które uniemożliwiają takie prawidłowe działanie.

Część II. Zasady wykonywania funkcji inspektora ochrony danych (IOD) określone w art. 38 ust. 6 RODO i cele ich wprowadzenia

Konstrukcja konfliktu interesów w działalności IOD została uregulowana w art. 38 ust. 6 RODO: „Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub

podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów".

Odnosząc treść art. 38 ust. 6 zd. drugie RODO do poczynionych w części I opinii, wniosków dotyczących rozumienia „konflikt interesów" należy przyjąć, że taki konflikt w przypadku inspektora ochrony danych (IOD) występuje w sytuacji, jeżeli inne nałożone na IOD zadania i obowiązki uniemożliwiają prawidłowe wykonywanie zadań IOD określonych w art. 39 RODO.

Prawodawca w art. 38 ust. 6 RODO jako źródło konfliktu interesów wskazuje wykonywanie innych zadań i obowiązków przez IOD, niż określone w art. 39 ust. 1 RODO, z tej przyczyny w niniejszej opinii odniesiono się wyłącznie do konfliktu interesów w rozumieniu ww. przepisu, nie odnosząc się przy tym do innych możliwych źródeł konfliktu interesów (np. zależności rodzinnych lub osobistych).

Występowanie konfliktu interesów w przypadku wykonywania funkcji IOD należy rozumieć wąsko. Konstrukcja art. 38 ust. 6 RODO wskazuje, że według prawodawcy unijnego zasadą jest możliwość wykonywania przez IOD dodatkowych zadań i obowiązków (zdanie pierwsze ust. 6). Natomiast wyjątkiem od tej zasady jest występowanie konfliktu interesów, któremu administrator (podmiot przetwarzający) powinien zapobiegać (zdanie drugie ust. 6). Występowanie konfliktu interesów jest zatem sytuacją wyjątkową, która uniemożliwia wykonywanie dodatkowych obowiązków i zadań przez IOD, podczas gdy taka dodatkowa aktywność jest co do zasady dopuszczalna. IOD jako osoba posiadająca odpowiednią wiedzę fachową z zakresu ochrony danych osobowych, będzie w ramach czynności doradczych wykonywać zadania związane z ochroną danych osobowych w organizacji, w szczególności, jeśli chodzi o IOD będącego członkiem personelu administratora[20]. Szczególnie w obszarze ochrony danych osobowych należy bowiem pamiętać, że głównym celem istnienia i aktywności IOD jest wsparcie administratora (podmiotu przetwarzającego) w realizacji jego obowiązków ustalonych w RODO, czemu może nawet sprzyjać nałożenie dodatkowych zadań na IOD.

Grupa Robocza Art. 29 w Wytycznych (243) twierdzi, że czynnikiem, który wskazuje na istnienie konfliktu interesów jest przede wszystkim ingerencja w niezależność wykonywania funkcji IOD. Zdaniem Grupy wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny, w związku z czym IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych osobowych (decydowanie o tych celach i sposobach)[21].

W ocenie autora opinii uznawanie istnienia konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO wyłącznie jako sytuacji, w której IOD decyduje o celach i sposobach przetwarzania w związku z wykonywaniem dodatkowych zadań obowiązków jest jednak zbyt zawężające. Uważam, że konflikt interesów w pełnieniu funkcji IOD występował będzie wtedy, gdy IOD z uwagi na realizację dodatkowych obowiązków lub zadań, nie będzie mógł wykonywać prawidłowo swoich zadań opisanych w art. 39 ust. 1 RODO, co może zaistnieć, gdy IOD decyduje o celach i sposobach przetwarzania danych osobowych, jednak nie tylko w takiej sytuacji. Przez prawidłowe wykonywanie zadań IOD rozumiem ich realizowanie w sposób:

- niezależny,
- obiektywny,

[20] Por. M. Hoskins, How to be a decent DPO: letters to aspiring privacy pros, 2021, str. 129.
[21] Wytyczne (243), str. 17.

- skuteczny.

Konflikt interesów zaistnieje natomiast, jeżeli jakiekolwiek inne wartości, czynniki lub interesy będą podważać którykolwiek z tych trzech aspektów wykonywania zadań IOD.

Zgodnie z art. 39 ust. 1 RODO do zadań, które IOD powinien wykonywać należą:

1) czynności informacyjno-doradcze dla wyznaczającego administratora (podmiotu przetwarzającego), w tym generalne działania informacyjne i doradcze w zakresie obowiązków spoczywających na administratorach, podmiotach przetwarzających i pracownikach (art. 39 ust. 1 lit. a RODO), a także konsultowanie oraz udzielanie zaleceń dla administratora co do oceny skutków dla ochrony danych (art. 35 ust. 2 i art. 39 ust. 1 lit. c RODO),
2) monitorowanie przestrzegania przepisów o ochronie danych osobowych i polityk w dziedzinie ochrony danych, ochrony danych osobowych (art. 39 ust.1 lit. b RODO)[22], w tym także monitorowania oceny skutków dla ochrony danych (art. 39 ust.1 lit. c RODO),
3) współdziałanie z organem nadzorczym, w tym współpraca z nim i pełnienie funkcji punktu kontaktowego dla tego organu (art. 39 ust. 1 lit d i e RODO).

Oczywiście wyjaśnienia wymagają trzy kluczowe cechy działalności IOD: **niezależność, obiektywizm i skuteczność**.

Pojęcie „**niezależności**" nie pojawia się bezpośrednio w przepisach RODO, ale w jednym z motywów preambuły tego aktu (motyw 74) i to w krótkim zdaniu, w którym stwierdza się: „Tacy inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny."[23]. Istotę niezależność ustala treść art. 38 ust.3 zd. pierwsze („Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań"). Wobec tego niezależność IOD będzie rozumiane jako niepodleganie inspektora instrukcjom co do merytorycznego wykonywania prawem określonych zadań. Pod względem podmiotowym ten brak podległości dotyczy instrukcji kierowanych od osób zarówno w sferze wewnętrznej jak i z zewnątrz jednostki organizacyjnej. Przekładając powyższe na pozytywne powinności niezależność sprowadza się do samodzielności inspektora w merytorycznej realizacji swoich zadań bez wpływu osób trzecich.

Z kolei **obiektywność** to „wyraz przedstawiania lub oceniania czegoś zgodnie z faktami, niezależnie od własnych poglądów lub emocji"[24]. IOD powinien dokonywać bowiem oceny wyłącznie w oparciu o własne wysokie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania własnych zadań, ponieważ takie są kryteria jego wyznaczenia (art 37 ust. 5 RODO).

Kryterium **skuteczności** oznacza, że działania IOD powinny być efektywne z punkty widzenia zasady ryzyka określonej w art. 39 ust. 2 RODO. IOD wypełnia swoje zadania z uwzględnieniem ryzyk związanych z operacjami przetwarzania danych, mając na uwadze

[22] Dodatkowo w art. 47 ust. 2 lit. h RODO przewidziano, że w przypadku przyjęcia wiążących reguł korporacyjnych do zadań IOD należy monitorowanie przestrzegania tych reguł oraz monitorowanie szkoleń i rozpatrywanie skarg.
[23] Motyw 74 zd. czwarte RODO.
[24] Wielki Słownik Języka Polskiego, hasło dostępne pod adresem URL: https://wsjp.pl/haslo/podglad/61398/obiektywnosc/5183897/oceny (dostęp: 5.04.2024 r.).

charakter, zakres, kontekst i cele przetwarzania. Powinno to prowadzić do aktywnej i zaangażowanej działalności IOD nastawionej na efektywność polegającą na zapewnieniu co najmniej należytego poziomu ochrony praw i wolności osób, których dane dotyczą, jak również wykonania obowiązków administratora (podmiotu przetwarzającego).

Biorąc pod uwagę zadania IOD oraz wyjaśnione powyżej cechy prawidłowości wykonywania zadań IOD konflikt interesów może zaistnieć ze względów:

- czasowych,

- ustrojowych,

- merytorycznych,

co szczegółowo wyjaśniono w dalszej części opinii.

Kwalifikację realizacji określonego, dodatkowego zadania przez IOD jako prowadzącego do wystąpienia konfliktu interesów, biorąc pod uwagę prawidłowość wykonywania przez IOD jego podstawowych zadań określonych w RODO, należy jednocześnie ujmować ostrożnie i wąsko. Przeciwne wnioskowanie spowodowałoby bowiem, że art. 38 ust. 6 *in principio* RODO stanowiłby normę pustą – pomimo formalnej dopuszczalności wykonywania innych zadań i obowiązków przez IOD, nie mógłby faktycznie realizować w organizacji jakichkolwiek innych zadań i obowiązków wykonywać. Co więcej, na konieczność takiej ostrożności wskazuje art. 39 ust. 1 lit. a RODO, zgodnie z którym do zadań IOD należy m. in informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

Kwestia doradzania administratorowi (podmiotowi przetwarzającemu) nieodłącznie wiąże się z zajmowaniem stanowiska, wyrażania poglądu lub opinii w określonej kwestii z obszaru ochrony danych osobowych w organizacji. Błędem byłoby tym samym wykładanie art. 39 ust. 1 lit. a) w zw. z art. 38 ust. 6 RODO w taki sposób, że zajęcie stanowiska przez IOD w kwestii przetwarzania danych osobowych w organizacji w ramach doradztwa, prowadzi do powstania konfliktu interesów. Istotne jest natomiast żeby IOD wyraził swoje stanowisko niezależnie, obiektywnie i skutecznie. Nie ma w efekcie znaczenia, czy administrator, korzystając z doradztwa IOD, zmodyfikuje proces przetwarzania danych osobowych, jak również to, że IOD w ramach art. 39 ust. 1 lit. b) RODO będzie monitorował ten proces.

Stwierdzenie występowania konfliktu interesów nie ma jednocześnie charakteru formalnego, co oznacza, że ma on związek z okolicznościami faktycznymi i dopiero ich ocena powoduje, że możliwe jest stwierdzenie czy konflikt interesów faktycznie występuje. W konsekwencji wykonywanie określonych przez IOD zadań w jednej organizacji będzie powodowało występowanie konfliktu interesów, podczas gdy to samo zadanie wykonywane w innych warunkach w innej organizacji nie będzie już powodowało takiego konfliktu. Każdorazowo zatem trzeba ocenić wpływ okoliczności realizowania zadań przez IOD na prawidłowość wykonywania tej funkcji. Znaczenie ma bowiem w jaki sposób w praktyce określone zadania powierzone IOD są przez niego wykonywane oraz w jakich okolicznościach ma to miejsce. Sygnalizuje to również Prezes UODO wskazując cyt. „Ocena, czy w przypadku konkretnej

osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana indywidualnie z uwzględnieniem konkretnych okoliczności."[25].

Potwierdza to też TSUE, który w wyroku z 9 lutego 2023 r. o sygn. C-453/21 stwierdził cyt. „konflikt interesów" (...) może istnieć w sytuacji, gdy inspektor ochrony danych otrzymuje inne zadania lub obowiązki, które prowadziłyby do określania przez niego celów i sposobów przetwarzania danych osobowych u administratora lub jego podmiotu przetwarzającego, co powinien ustalić sąd krajowy odrębnie dla każdego przypadku **na podstawie oceny wszystkich istotnych okoliczności**, w szczególności struktury organizacyjnej administratora lub jego podmiotu przetwarzającego, oraz w świetle całości obowiązujących przepisów, w tym ewentualnych przepisów wewnętrznych administratora lub podmiotu przetwarzającego.".

Konflikt interesu w działalności IOD nie ma przy tym charakteru stopniowalnego – co oznacza, że albo on występuje albo nie[26]. Konflikt interesów ma przy tym charakter obiektywny[27] - odwoływanie się do subiektywnego postrzegania inspektora ochrony danych nie odzwierciedlałoby wszystkich okoliczności możliwego konfliktu interesów.

Znamienne jest przy tym, że zarówno Grupa Robocza Art. 29 w Wytycznych (243) jak i EROD w Raporcie nie przesądzają jednoznacznie, że wykonywanie konkretnego zadania lub zajmowanie określonego stanowiska zawsze będzie powodowało konflikt interesów IOD. W ww. dokumentach wskazano natomiast, że konflikt interesów **może występować,** jeżeli wykonywanie dodatkowych zadań przez IOD lub zajmowanie określonego stanowiska w organizacji, będzie związane z decydowaniem o celach i sposobach przetwarzania danych osobowych[28].

Powyższe koresponduje zatem z twierdzeniem autora niniejszej opinii, że występowanie konfliktu interesów stanowi okoliczność obiektywną, uzależnioną od elementów stanu faktycznego, związanego z rodzajem i sposobem wykonywania zadań przekazanych do realizacji przez IOD, które chociaż potencjalnie mogą mieć wpływ na prawidłowość wykonywania zadań opisanych w art. 39 ust. 1 RODO.

Rodzaje konfliktów interesów w ochronie danych osobowych

Mając na uwadze trzy aspekty prawidłowości wykonywania zadań IOD (tj. niezależność, obiektywizm oraz skuteczność) w kontekście potencjalnego występowania konfliktu interesów w sprawowaniu funkcji IOD w rozumieniu art. 38 ust. 6 RODO, możliwe jest rodzajowe wyodrębnienie trzech aspektów ww. konfliktu interesów:

1) Konflikt interesów o charakterze ustrojowym, mający wpływ na niezależność wykonywania funkcji IOD,
2) Konflikt interesów o charakterze merytorycznym, mający wpływ na obiektywizm i niezależność wykonywania funkcji IOD,
3) Konflikt interesów o charakterze czasowym, mający wpływ na skuteczność wykonywania funkcji IOD.

[25] Komunikat z 3 listopada 2021 r. Prezesa UODO dostępny pod adresem URL: https://uodo.gov.pl/pl/495/2415 (dostęp: 5.04.2024 r.).
[26] Ibidem, str. 22 – 23.
[27] Tak również: P. Grosmann, Die Interessenkonflikte der betrieblichen und behördlichen Datenschutzbeauftragten. Springer, Berlin, Heidelberg 2024, https://doi.org/10.1007/978-3-662-68387-3_1, str. 59.
[28] Raport str. 24, Wytyczne (243) str. 17.

Poniżej przedstawiono charakterystykę każdego z ww. rodzajów konfliktów interesów.

Konflikt interesów o charakterze ustrojowym

Konflikt interesów w aspekcie ustrojowym polega na takim usytuowaniu IOD w organizacji, że nie podlega on wyłącznie najwyższemu kierownictwu, który to wymóg wprowadza art. 38 ust. 3 RODO. Wymóg ten pozostaje aktualny również w przypadku zlecenia IOD wykonywania dodatkowych zadań lub obowiązków.

RODO nie definiuje pojęcia najwyższego kierownictwa, należy jednak przyjąć, że jest to osoba albo grupa osób, które kierują organizacją, wskazują strategiczne cele i misję jej działania oraz nadzorują działania organizacji, czyli np. zarząd spółki kapitałowej, piastun organu administracyjnego[29].

Osoba kontrolująca pracę IOD w obszarze wykonywania przez niego dodatkowych obowiązków, może potencjalnie próbować wykorzystać tę zależność w celu wpłynięcia na ocenę przez IOD kwestii związanych z ochroną danych osobowych w komórce organizacyjnej, nadzorowanej przez ww. osobę – co godzić będzie w niezależność IOD. Inspektor ochrony danych, który w ramach wykonywania dodatkowych zadań podlega służbowo oraz ocenie innej osoby w organizacji, niż najwyższe kierownictwo może odczuwać nacisk, by współpracować i mieć dobre relacje z kierownictwem i innymi pracownikami, co może mieć wpływ na prawidłowe realizowanie podstawowych zadań IOD[30].

O ile nie można definitywnie *a priori* stwierdzić, że nie jest możliwe wykonywanie dodatkowych zadań IOD, pod kontrolą innej niż najwyższe kierownictwo osoby z organizacji, to przewidzenie odpowiednich mechanizmów gwarantujących taką niezależność, również mając na uwadze rodzaj dodatkowych zadań, będzie utrudnione.

W konsekwencji w ocenie autora opinii, jeżeli IOD zostaną zlecone w organizacji inne zadania, niż opisane w art. 39 ust. 1 RODO, to powinien on odpowiadać za ich wykonywanie przed najwyższym kierownictwem podmiotu, który go powołał do wykonywania funkcji IOD.

Konflikt interesów o charakterze merytorycznym

Konflikt interesów o charakterze merytorycznym może być związany z następującymi okolicznościami:

1) IOD decyduje o celach i sposobach przetwarzania danych, w tym poprzez zastępowanie administratora w sposób formalny lub materialny w realizacji obowiązków dotyczących przetwarzania danych osobowych;

2) IOD pełni swoją funkcję jednocześnie w przynajmniej dwóch podmiotach pozostających ze sobą w relacji, związanej z udostępnianiem danych osobowych jako odrębni od siebie administratorzy danych osobowych (z wyłączeniem grupy przedsiębiorców) lub jako administrator oraz podmiot przetwarzający.

Decydowanie o celach i sposobach przetwarzania danych osobowych

[29] E. Bielak-Jomaa, [w:] E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, LEX, 2018, art. 38.
[30] Ibidem.

Decydowanie o celach i sposobach przetwarzania będzie powodowało konflikt interesów o charakterze merytorycznym. Jednocześnie podejmowanie takich decyzji jest związane z zajmowaniem określonych stanowisk w organizacji. Z tej przyczyny Grupa Robocza Art. 29 w Wytycznych (243) wskazała, że IOD nie powinien zajmować stanowisk kierowniczych; z nimi bowiem związane jest podejmowanie ww. decyzji lub udział w ich podejmowaniu[31]. Głównym kryterium oceny w przypadku tego rodzaju konfliktu interesów jest jednak nie sam fakt piastowania określonego stanowiska, a możliwość podejmowania decyzji co do celów i sposobów przetwarzania danych osobowych[32].

Decydowanie o celach i sposobach przetwarzania danych osobowych przez IOD powoduje, że nie może on obiektywnie, następczo ocenić prawidłowości działań administratora, skoro samodzielnie dokonywał ich w jego imieniu. Ponadto decydowanie o celach i sposobach przetwarzania danych osobowych jest elementem identyfikującym administratora danych osobowych, zgodnie z definicją opisaną w art. 4 pkt 7 RODO. Oznacza to, że m. in. zlecenie IOD decydowania o realizacji praw osób, których dane dotyczą, samodzielne opracowywanie i wdrażanie rozwiązań dotyczących przetwarzania danych osobowych w organizacji, udzielanie upoważnień do przetwarzania danych osobowych, pełnienie roli pełnomocnika administratora (podmiotu przetwarzającego) w postępowaniu, będzie prowadziło do konfliktu interesów.

Konflikt ten oznacza bowiem, że IOD nie może obiektywnie ocenić procesu przetwarzania danych osobowych w ramach zadań przewidzianych w art. 39 ust. 1 RODO, a zatem jego realizacja powodować będzie konflikt interesów.

Pełnienie funkcji IOD w dwóch podmiotach o sprzecznych interesach

Powodem występowania konfliktu interesów o charakterze merytorycznym potencjalnie może być pełnienie przez IOD swojej funkcji w więcej niż jednej organizacji. Z perspektywy administratora (podmiotu przetwarzającego) dodatkowymi zadaniami i obowiązkami, o których mowa w art. 38 ust. 6 RODO będą bowiem również, realizowane przez w organizacji innego administratora lub podmiotu przetwarzającego.

Ryzyko powstania konfliktu interesów może więc wystąpić, jeżeli oba podmioty, w których IOD pełni swoją funkcję, nawiążą relację prawną, wymagającą doradzania przez IOD obu stronom stosunku prawnego, co do tych samych okoliczności. IOD powinien doradzać administratorowi z perspektywy prawidłowości przetwarzania danych osobowych w jego organizacji i zabezpieczenia jego interesów w tym kontekście, czego nie można pogodzić z tożsamym doradztwem na rzecz innego podmiotu w ramach tego samego stosunku prawnego[33]. Może zatem dojść do potencjalnego uchybienia w obszarze niezależności i obiektywizmu IOD.

Jednocześnie należy zauważyć, że art. 37 ust. 2 RODO dopuszcza powołanie jednego IOD dla grupy przedsiębiorstw, w związku z czym w takiej sytuacji nie będzie dochodziło do konfliktu interesów. Jest to uzasadnione, ponieważ grupa przedsiębiorstw, pomimo iż w jej skład wchodzą odrębni od siebie administratorzy danych osobowych, to pozostają oni w takiej relacji, że ich cele i działania są wspólne i powiązane ze sobą, z uwagi na sprawowanie kontroli przez jeden z tych podmiotów nad pozostałymi z grupy (art. 4 pkt 19 RODO).

Podobnie art. 37 ust. 3 RODO, jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z

[31] Wytyczne (243), str. 25.
[32] Ibidem
[33] Raport, str. 25-26.

uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych. Wydaje się, że powołanie tego samego IOD w przypadku podmiotów publicznych byłoby możliwe, w przypadku jednostek organizacyjnych jednostek samorządu terytorialnego, powołanych do realizacji określonych zadań (np. gminy), których sposób działania i realizacja zadań nie zostały odrębnie przewidziane w powszechnie obowiązujących przepisach prawa. Głównym kryterium, które powinno być wzięte pod uwagę dla oceny możliwości takiego powołania jest jednak prawidłowość wykonywania zadań przez IOD. Jak wskazuje się bowiem w doktrynie „Jeden inspektor wyznaczony np. dla kilku ministerstw nie zawsze będzie mógł realizować swoje zadania w sposób właściwy, biorąc pod uwagę różne cele i zakres działań różnych ministerstw.[34]".

Konflikt interesów o charakterze czasowym

Konflikt interesów może być wynikiem nadmiaru innych obowiązków (zadań) powierzonych do realizacji inspektorowi ochrony danych w sytuacji, gdy inspektor będzie musiał wybierać, które z obowiązków będzie wykonywał, a którego wykonać nie zdoła ze względu na brak czasu potrzebnego na jego realizację[35].

Konflikt interesów o charakterze czasowym oznacza, że IOD nie może zatem wykonywać skutecznie swoich zadań – nałożenie na niego dodatkowych zadań lub obowiązków może spowodować, że w przypadku części lub całości zadań przewidzianych w art. 39 ust. 1 RODO działa jedynie reaktywnie. Reaktywność działań oznacza, że IOD z powodu czasu nie ma możliwości wykonywania swoich zadań w sposób w pełni inicjujący i aktywny, ale skupi się jedynie na swoich podstawowych obowiązkach. Wówczas administrator (podmiot przetwarzający) nie otrzymuje niezbędnych informacji i wskazówek w obszarze ochrony danych osobowych w organizacji, przez co powołanie IOD nie zapewnia wyższego standardu ochrony danych osobowych. W ten sposób IOD nie wykonuje bowiem faktycznie swoich zadań. Zauważyć przy tym trzeba, że RODO zakłada ochronę danych osobowych prowadzoną w oparciu o ryzyko wystąpienia negatywnych zdarzeń mogących naruszać prawa i wolności osób, których dane dotyczą. Obowiązki administratora (podmiotu przetwarzającego) polegają w dużej mierze na zapobieganiu i przeciwdziałaniu zarówno samym zdarzeniom zagrażającym danym osobowym w organizacji jak i organizowaniu przetwarzania danych osobowych w taki sposób, żeby przed jego rozpoczęciem zminimalizować ryzyko wystąpienia negatywnych skutków na podmiotów danych (m. in. art. 24, 25, 32, 35, 36 RODO).

Podejście oparte na ryzyku przewidziane w RODO wyklucza możliwość ograniczenia aktywności IOD wyłącznie do reagowania na zdarzenia w organizacji. Przekłada się to na brak skuteczności IOD w realizacji swoich zadań. Takie ograniczenie będzie powodowało wystąpienie konfliktu interesów o charakterze czasowym.

Trzeba przy tym zaznaczyć, że RODO nie przewiduje ograniczenia co do liczby podmiotów, w których IOD może pełnić swoją funkcję, jak również co do przedmiotu ich działalności czy wielkości. Niezależnie bowiem od tych czynników istotne jest, aby rola IOD nie ograniczała się jedynie do pozostawania wyłącznie osobą wyznaczoną do realizacji zadań opisanych w art. 39 ust. 1 RODO, podczas gdy zadania te są realizowane bez udziału IOD przez inne podmioty.

[34] E. Bielak-Jomaa [w:] D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, art. 37.
[35] P. Fajgielski, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II, Warszawa 2022, art. 38.

Zaznaczyć trzeba, że to sam IOD powinien decydować o ostatecznym kształcie m. in. rekomendacji czy wniosków z przeprowadzonego audytu. Jeżeli IOD jest wspierany w wykonywaniu zadań przez wyznaczony do tego zespół osób, to jego rolą jest również aktywnie koordynować pracę tego zespołu, biorąc w niej bezpośredni udział i podejmując decyzje co do kierunków prac oraz wniosków i propozycji przedstawianych administratorowi. Należy bowiem zaznaczyć, że wykonywanie zadań IOD nie musi oznaczać realizacji przez IOD każdej czynności w ramach tego zadania. Istotne jest jednak, żeby to IOD ostatecznie podejmował decyzję o kształcie rekomendacji, czy zakresie dokonywanych sprawdzeń u administratora w ramach prowadzonych audytów. Powyższe znajduje potwierdzenie w stanowisku Grupy Roboczej Art. 29 wyrażonym w Wytycznych (243), zgodnie z którym: „W zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych (IOD i jego pracowników). W przypadku powołania takiego zespołu, jego struktura, podział i zakres obowiązków powinny zostać jasno ustalone. Również w przypadku wyznaczenia IOD spoza organizacji, zespół pracowników podmiotu zewnętrznego powołany do wypełniania obowiązków związanych z ochroną danych osobowych może efektywnie wypełniać zadania IOD, gdy wyznaczona zostanie osoba odpowiedzialna za kontakt z klientem”.

O konflikcie interesów o charakterze czasowym nie świadczy zatem, czy IOD samodzielnie wykonuje wszystkie czynności (w tym czynności techniczne) związane z realizacją swoich zadań, ale czy jest on w stanie korzystając z pomocy zespołu, pełnić swoją funkcję aktywnie i skutecznie, podejmując ostateczne decyzje i odpowiadać za końcowy kształt i sposób podejmowanych działań, opracowywanych treści lub kierowanych do administratora (podmiotu przetwarzającego) zaleceń oraz rekomendacji.

Unikanie konfliktu interesów w działalności IOD

Zarówno administrator jak i podmiot przetwarzający są podmiotami, które zgodnie z art. 38 ust. 6 zd. drugie RODO są zobowiązane do zapewnienia, żeby dodatkowe zadania i obowiązki IOD nie powodowały występowania konfliktu interesów.

Podmiot wyznaczający IOD ponosi odpowiedzialność za to, aby zarówno w momencie wskazania konkretnej osoby do pełnienia funkcji IOD, jak i przez cały okres pełnienia przez nią tej funkcji nie dochodziło do konfliktu interesów. Chociaż przeciwdziałanie występowaniu konfliktu interesu stanowi bezpośredni obowiązek podmiotu, to w praktyce przeciwdziałanie temu konfliktowi będzie utrudnione lub nawet niemożliwe bez aktywnego udziału IOD. IOD nie może bowiem pełnić swojej funkcji w sposób prawidłowy w warunkach występowania konfliktu interesów – powinien on zatem informować podmiot, który go wyznaczył, o istnieniu konfliktu interesów.

Wymóg unikania konfliktu interesów polega na prowadzeniu rozwiązań w organizacji, które będą zapewniać, że IOD będzie wykonywał swoje zadania w sposób niezależny, obiektywny i skuteczny. Zasady przyjęte w organizacji powinny umożliwiać rozpoznanie okoliczności mogących powodować występowanie konfliktu interesów oraz odpowiednią reakcję na ten konflikt[36].

W przepisach RODO nie wskazano konkretnych rozwiązań, sposobów postępowania, które administrator powinien wdrożyć, aby skutecznie uniknąć konfliktu interesów w działalności

[36] Decyzja belgijskiego organu nadzorczego w sprawie Proximus z dnia 28 kwietnia 2020 r.

IOD. Grupa Robocza Art. 29 jako potencjalne rozwiązania, które administrator może zastosować w tym zakresie, wskazuje m. in.:

- określenie stanowisk powodujących konflikt z funkcją IOD;

- opracowanie wewnętrznych zasad pozwalających uniknąć konfliktu interesów;

- zadeklarowanie, przez IOD, że nie ma konfliktu interesów w odniesieniu do pełnionej przez siebie funkcji IOD;

- wprowadzenie zabezpieczeń do wewnętrznych zasad organizacji;

- zapewnienie, by ogłoszenie o naborze na stanowisko IOD lub umowa o świadczenie usług były wystarczająco jasne i precyzyjne[37].

Należy podkreślić, że katalog rozwiązań wskazanych przez Grupę Roboczą Art. 29 ma charakter otwarty, a organizacje decydując o metodach przeciwdziałających występowaniu konfliktu interesów powinny we własnym zakresie uwzględnić wewnętrzne zasady i dotychczasowe dobre praktyki podejmowane dla przeciwdziałania konfliktom interesu w przypadku innych stanowisk.

Zasady postępowania mające na celu uniknięcie konfliktu interesu o charakterze ustrojowym skupiają się przede wszystkim na zapewnieniu, że w sposób wykonywania zadań opisanych w 39 ust. 1 RODO przez IOD nie będą ingerowały osoby trzecie, którym IOD miałby podlegać w związku z realizacją dodatkowych zadań. W celu uniknięcia tego rodzaju konfliktu interesów rekomendowanym rozwiązaniem jest podleganie przez IOD najwyższemu kierownictwu, również w przypadku realizacji dodatkowych zadań zleconych inspektorowi.

Środki mające przeciwdziałać występowaniu konfliktu interesu o charakterze merytorycznym powinny zapewniać, aby IOD nie wykonywał dodatkowych zadań związanych z decydowaniem przez niego o celach i sposobach przetwarzania danych. IOD musi być jednak włączany we wszystkie sprawy związane z ochroną danych osobowych w organizacji. Oznacza to, że IOD może przedstawiać pewne rekomendacje rozwiązań, jednak nie powinien formalnie i faktycznie decydować o kwestiach związanych z przetwarzaniem danych osobowych w organizacji, w tym określaniu podstaw prawnych przetwarzania danych, usuwaniu danych, okresach retencji, realizacji praw osób, których dane dotyczą, reprezentowaniu administratora (podmiotu przetwarzającego) w postępowaniu. Natomiast jeżeli IOD pełni swoją funkcję w więcej niż jednym podmiocie, powinien zostać zobowiązany do informowania administratora (podmiot przetwarzający) o możliwości wystąpienia konfliktu interesów, z uwagi na pełnienie tej funkcji w innym podmiocie.

Środki podejmowane dla uniknięcia czasowego konfliktu interesu powinny zagwarantować, że IOD będzie dysponował odpowiednimi zasobami czasowymi, aby skutecznie wykonywać swoje zadania opisane w art. 39 ust. 1 RODO.

W przypadku IOD wykonującego zadania na podstawie umowy o pracę rozwiązaniem może być wydłużenie godzin pracy IOD (np. zwiększenie wymiaru etatu) lub zapewnienie IOD zespołu osób, które będą wpierać IOD w wykonywaniu jego zadań oraz zadań dodatkowych. Należy przy tym mieć na uwadze, że pracownik nie może być zobowiązany do wykonywania pracy, której wykonanie nie jest możliwe w ramach przypisanego mu wymiaru czasu pracy; jeżeli zatem wymiar czasu pracy pracownika stanowi 40 godzin tygodniowo i w danym przypadku nie jest wystarczającego do wykonania zleconych mu zadań, to zwiększenie

[37] Wytyczne (243), str. 19-20.

wymiaru czasu pracy nie może być odpowiedzią na ww. konflikt. Konieczne może okazać się zapewnienie dodatkowych zasobów osobowych przez administratora (podmiot przetwarzający) tak, by ww. zadania IOD mogły być realizowane lub przeniesienie niektórych dodatkowych zadań zleconych IOD na inną osobę w organizacji.

Należy jednak zauważyć, że konflikt interesów o charakterze czasowym może wystąpić również w przypadku, gdy IOD nie jest członkiem personelu administratora (podmiotu przetwarzającego) i jest podmiotem zewnętrznym świadczącym usługi na podstawie umowy cywilnoprawnej. Podkreślenia jednak wymaga, że zaangażowanie IOD i jego dyspozycyjność dla administratora (podmiotu przetwarzającego) stanowi istotny element stosunku zobowiązaniowego. Oznacza to, że w takim przypadku narzędzia niezbędne do wykonania umowy, w tym odpowiednie kompetencje i kwalifikacje do wykonania przedmiotu umowy obciążają stronę, która zobowiązała się do wykonania określonego świadczenia.

Jednocześnie, o czym należy pamiętać, istotą umowy cywilnoprawnej, jest zapewnienie przez stronę realizującą zlecenie lub usługę niezbędnych zasobów i środków do ich wykonania. W przypadku umowy o charakterze cywilnoprawnym to zleceniobiorca musi zapewnić możliwość i zdolność do wykonywania zlecenia. Środkiem służącym unikaniu konfliktu interesów o charakterze czasowym w przypadku zawierania umowy z podmiotem zewnętrznym jest zatem sam fakt wyboru umowy, na podstawie której świadczona będzie usługa oraz jej postanowienia.

Część III. Dodatkowe zadania i obowiązki IOD

Jak wskazano w art. 38 ust. 6 zd. pierwsze RODO inspektor ochrony danych może wykonywać inne zadania i obowiązki niż opisane w art. 39 ust. 1 RODO. Nie wszystkie dodatkowe zadania IOD będą dotyczyć obszaru ochrony danych osobowych, choć z uwagi na wiedzę fachową i specjalizację IOD, administrator lub podmiot przetwarzający mogą zlecać dodatkowe zadania IOD również związane z wykonywaniem obowiązków przewidzianych w RODO.

Należy przy tym pamiętać, że IOD powinien być włączany we wszystkie kwestie dotyczące ochrony danych osobowych. Brak konsultacji z IOD lub jego udziału w ww. kwestiach oznaczał będzie uchybienie wymogom art. 38 ust. 1 RODO. Udział IOD, również na etapie projektowania procesu przetwarzania, będzie miał lub może mieć wpływ na ostateczny kształt przyjętego w wyniku udziału lub konsultacji rozwiązania albo procesu przetwarzania danych. Należy jednak zaznaczyć, że to nie IOD powinien decydować o ostatecznym kształcie środków i rozwiązań przyjętych w organizacji administratora (podmiotu przetwarzającego) – IOD nie powinien bowiem określać celów i sposobów przetwarzania danych osobowych w organizacji. Prawodawca nie wskazał jednak, że administrator (podmiot przetwarzający) nie może zlecić IOD dodatkowych zadań związanych z realizacją przez administratora (podmiot przetwarzający) obowiązków przewidzianych w RODO. Jedyną przeszkodą dla zlecenia dodatkowych zadań i obowiązków IOD jest występowanie konfliktu interesów, który uniemożliwia wykonywanie zadań IOD w sposób prawidłowy, tj. niezależny, obiektywy oraz skuteczny.

Co prawda, Prezes UODO w treści jednego z Biuletynów UODO[38] wskazuje, że IOD nie może podejmować się żadnych zadań, które na mocy RODO są przypisane administratorowi

[38] Biuletyn UODO nr 2/04/23, str. 10.

(podmiotowi przetwarzającemu) (choć pierwotnie prezentował odmienne stanowisko[39]), to pomija on, że IOD oraz administrator (podmiot przetwarzający) nie są odrębnymi i niezależnymi od siebie podmiotami przetwarzającymi dane osobowe (administratorami, podmiotami przetwarzającymi, odbiorcami danych). Nieuzasadnione jest zatem wywodzenie, że skoro prawodawca w treści przepisu wskazał, iż jakiś obowiązek spoczywa na administratorze (podmiocie przetwarzającym), to z tej przyczyny nie jest możliwe zlecenie jego realizacji IOD.

Podkreślić trzeba, że administrator (podmiot przetwarzający) odpowiada za działania IOD i nie jest możliwe przeniesienie bezpośredniej odpowiedzialności za jakiekolwiek nieprawidłowości w obszarze wykonywania swoich obowiązków na IOD. Co więcej, to administrator (podmiot przetwarzający) decyduje wewnętrznie w organizacji jaka osoba (pracownik lub współpracownik) będzie podejmowała określone czynności, w tym będzie faktycznie realizowała obowiązki nałożone na administratora (podmiotu przetwarzającego) w RODO. Działanie pracownika podmiotu w ramach obowiązków służbowych i z polecenia pracodawcy nie powinno być oceniane jako działanie pracownika, odrębne od samego pracodawcy. Jest to szczególnie widoczne w przypadku podmiotów posiadających odrębną osobowość prawną takie jak np. spółki kapitałowe, fundacje czy stowarzyszenia. Pomimo tego, że faktyczna odpowiedzialność za realizację obowiązków przewidzianych w RODO spoczywa na osobie prawnej, to w praktyce nie ma faktycznej możliwości, by taki podmiot dokonywał poszczególnych czynności faktyczne samodzielnie; rzeczywiście realizują je bowiem zatrudnieni w podmiocie pracownicy. Nie można zatem przyjąć, że administrator (podmiot przetwarzający) nie wykonuje określonego obowiązku w sposób prawidłowy z samego faktu, że czynności faktycznej dokonuje pracownik takiego podmiotu – takie działanie będzie bowiem naturalnym środkiem realizacji obowiązku. Co więcej, takim pracownikiem potencjalnie może być również IOD; brak jest bowiem wyłączenia w tym zakresie w przepisach powszechnie obowiązującego prawa. Nawet jeżeli działania IOD są realizowane w oparciu o umowę z podmiotem zewnętrznym, to w dalszym ciągu administrator (podmiot przetwarzający) odpowiada zarówno przed podmiotami danych jak i przed organem nadzorczym, za realizację obowiązków opisanych w RODO, w tym również za ewentualne błędy i nieprawidłowości w obszarze ochrony danych osobowych. Z samego tylko faktu zlecenia przez administratora (podmiot przetwarzający) realizacji określonego obowiązku podmiotowi trzeciemu nie można wywodzić, że administrator (podmiot przetwarzający) zaprzestał wykonywania tego obowiązku lub że zlecenie tego zadania IOD w ramach umowy outsourcingu jest niedopuszczalne.

Jeżeli zatem prawodawca przypisał zadanie administratorowi lub podmiotowi przetwarzającemu, to nie oznacza, że IOD z tego właśnie powodu nie może ich realizować w organizacji. Przeszkodą w wykonywaniu takiego zadania będzie dopiero wystąpienie konfliktu interesów w rozumieniu art. 38 ust. 6 RODO, który został już omówiony w treści opinii.

Udział IOD w tworzeniu dokumentacji przetwarzania danych osobowych

Zauważyć trzeba, że formalnie RODO wymaga prowadzenia ograniczonego zakresu dokumentacji dotyczącej przetwarzania danych osobowych w organizacji, wskazując jedynie na dwa dokumenty i precyzując ich zawartość, tj. RCP (art. 30 ust. 1 RODO) oraz RCKP (art. 30 ust. 2 RODO).

[39] Komunikat z 15.01.2019 Prezesa UODO dostępny pod adresem URL: https://archiwum.uodo.gov.pl/pl/225/659 (dostęp: 5.04.2024 r.).

Administrator ma również obowiązek dokumentowania zaistniałych w organizacji naruszeń (art. 33 ust. 5 RODO), choć prawodawca nie wskazuje formy, w jakiej powinno się to odbywać oraz dokładnej (pełnej) treści, która powinna być gromadzona w celu wykonania tego obowiązku.

RODO sygnalizuje również, choć pośrednio, udokumentowany charakter DPIA oraz wskazuje na obowiązek konsultowania się z IOD w ramach jej prowadzenia (art. 35 ust. 2 RODO).

Prowadzenie pozostałej dokumentacji, wykraczającej poza ww. zakres jest zasadne i obliczone na rozliczalność działań administratora (podmiotu przetwarzającego), aby móc wykazać organowi nadzorczemu, że pozostaje on w zgodzie z postanowieniami RODO. Brak jest jednak wskazówek prawodawcy w tym zakresie oraz brak jest wymogów co powinny zawierać te dodatkowe dokumenty, jak również brak wskazania jakie dokumenty administrator (podmiot przetwarzający) powinien jeszcze posiadać.

Powstaje zatem pytanie, czy IOD może, działając na polecenie administratora lub podmiotu przetwarzającego prowadzić odpowiednio RCP lub RCKP oraz dokumentować zaistniałe w organizacji naruszenia i brać aktywny udział w przeprowadzeniu oceny skutków dla ochrony danych osobowych.

Prowadzenie przez IOD RCP oraz RCKP

Czynności dokumentacyjne, zmierzające do potwierdzenia istniejącego stanu faktycznego, tj. czynności o charakterze deklaratoryjnym, nie mają związku z decydowaniem o celach i sposobach przetwarzania danych osobowych, a tym samym nie mają ona wpływu na prawidłowość wykonywania zadań przez IOD. Jeżeli jednak w danej organizacji czynność dokumentacyjna ma mieć charakter konstytutywny, tj. przy jej dokonywaniu dochodzi do określania celów i sposobów przetwarzania danych osobowych w tym np. decydowania o podstawie prawnej przetwarzania lub określania w jaki sposób dane osobowe są przetwarzane w organizacji – to w takim przypadku dokonywanie tej czynności będzie powodowało występowanie konfliktu interesów funkcji IOD.

Należy zwrócić uwagę, że prowadzenie RCP oraz RCKP ma charakter dokumentacyjny. Ich prowadzenie polega na odzwierciedleniu i utrwaleniu rzeczywistego stanu faktycznego w organizacji. Brak jest przy tym decydowania o celach i sposobach przetwarzania danych osobowych, w związku z czym co do zasady, prowadzenie tego rodzaju dokumentów nie będzie prowadziło do powstawania konfliktu interesów w wykonywaniu funkcji IOD.

W doktrynie przyjmuje się również, że prowadzenie RCP związane jest z rolą IOD jako podmiotu, który wspiera administratora w zachowaniu zgodności z wymogami określonymi w przepisach o ochronie danych osobowych[40]. Inspektor ochrony danych, zwłaszcza w mniejszych organizacjach, będzie zwykle jedyną kompetentną osobą, która może prowadzić rejestr czynności przetwarzania spełniający wymogi RODO. Dokumentowanie operacji przetwarzania przez inspektora ochrony danych nie uniemożliwia monitorowania administratora w zakresie spełnienia samych obowiązków określonych w RODO[41].

[40] C. Àlvarez Rigaudias, A. Spina, Article 39: Tasks of The Data Protection Officer, [w:] The EU General Data Protection Regulation (GDPR): A Commentary, C. Kuner, L.A. Bygrave, C. Docksey (red.), Oxford 2020, s. 710–711.
[41] P. Grosmann, Die Interessenkonflikte der betrieblichen..., str. 58

Zauważyć przy tym trzeba, że jeszcze pod rządami Dyrektywy 95/46/WE oraz Ustawy z 1997 r. zadaniem osoby pełniącej funkcję administratora bezpieczeństwa informacji (ABI) (poprzednika IOD) było prowadzenie rejestru operacji przetwarzania danych osobowych (tak art. 18 ust. 2 tiret 4 Dyrektywy 95/46/WE). Rejestr ten, w Ustawie z 1997 r. nazywany był rejestrem zbiorów danych (art. 36a Ustawy z 1997 r.). Chodzi o ostateczny kształt funkcji ABI ustalony nowelizacją z 2014 r. ustawy o ochronie danych osobowych (1997 r.) (tj. ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej, Dz.U. z 2014 r., poz. 1662), która obowiązywała od 1 stycznia 2015 r. Jednym z celów tych zmian ustawowych z 2014 r. było przygotowanie ABI do wykonywania funkcji IOD, a zgodnie z art. 36a ust.8 tejże ustawy ABI miał mieć zapewnione środki i organizacyjną odrębność niezbędne do niezależnego wykonywania przez niego zadań.

Zgodnie natomiast z rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015 poz. 719, uchylone), rejestr zbiorów danych osobowych zawierał m. in. podstawę prawną upoważniającą do prowadzenia zbioru danych; cel przetwarzania danych w zbiorze; opis kategorii osób, których dane są przetwarzane w zbiorze; zakres danych przetwarzanych w zbiorze; oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane; informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego (§3).

Odpowiednikiem rejestru zbiorów danych osobowych pod rządami ustawy z 1997 r. jest zatem w pewnym zakresie rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO. Zauważyć trzeba, że w RCP znajdują się, poza informacjami identyfikującymi IOD i Administratora, informacje o celach przetwarzania; opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych; jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Porównując zakres informacji, który znajduje się w RCP, z tym, który ABI powinien zawrzeć prowadząc rejestr zbiorów danych osobowych należy uznać, że rejestr prowadzony pod rządami ustawy z 1997 r. zawiera szerszy katalog informacji niż RCP. Racjonalny ustawodawca nie mógłby zatem z jednej strony gwarantując ABI niezależność, zobowiązywać go do podejmowania działań skutkujących konfliktem interesów. Jak wskazano powyżej, zarówno w przypadku prowadzenia RCP, jak i rejestru zbiorów danych nie występuje i nie występował konflikt interesów.

Podobnie twierdził Generalny Inspektor Ochrony Danych Osobowych, który w urzędowej publikacji z 2016 r. wskazał na bezpośrednie podobieństwo pomiędzy dotychczas prowadzonym przez ABI rejestrem zbiorów danych, a RCP na podstawie art. 30 RODO: „Przepisem RODO zobowiązującym administratorów danych i podmioty przetwarzające do wprowadzenia takiej inwentaryzacji jest art. 30 RODO dotyczący rejestrowania czynności przetwarzania. Przepis ten, podobnie jak obecnie obowiązująca Ustawa z 1997 r., w szczególnych przypadkach wymaga prowadzenia rejestru czynności przetwarzania danych osobowych. **Jego zawartość przypomina rejestr zbiorów danych osobowych, do prowadzenia, którego zobowiązani są obecnie ABI**. Wprowadzony w RODO tzw. rejestr

czynności przetwarzania należy rozumieć jako wykaz przetwarzanych zbiorów danych, na które dzieli się wszystkie przetwarzane u danego administratora danych."[42].

Skoro zatem prowadzenie rejestru zbiorów danych osobowych w oparciu o Dyrektywę 95/46/WE oraz Ustawę z 1997 r., zawierającego więcej informacji niż obecnie prowadzony RCP na podstawie RODO nie powodowało występowania konfliktu interesów w sprawowaniu funkcji ABI, to nieuzasadnionym jest uznanie, że prowadzenie RCP przez IOD stanowi o występowaniu konfliktu interesów pod rządami RODO. Występowanie konfliktu interesów stanowi bowiem okoliczność faktyczną o charakterze obiektywnym. Zauważyć natomiast należy, że IOD może wykonywać inne zdania niż przewidziane jako obowiązkowe do wykonywania zgodnie z art. 39 RODO, jeżeli nie zachodzi konflikt interesów powodujący brak takiej możliwości.

Oznacza to, że zarówno w czasie obowiązywania Dyrektywy 95/46/WE jak i od chwili stosowania RODO prowadzenie rejestru operacji przetwarzania danych osobowych, czy to w postaci rejestru zbiorów danych osobowych (przed 25 maja 2018 r.), czy w postaci rejestru czynności przetwarzania danych osobowych (po 25 maja 2018 r.) przez ABI (przed 25 maja 2018 r.) lub IOD (po 25 maja 20218 r.) nie powodowało i nie powoduje konfliktu interesów.

Na dopuszczalność prowadzenia przez IOD RCP w imieniu administratora w związku z pełnieniem jego roli w organizacji wskazuje wprost Grupa Robocza Art. 29, według której cyt. "nic nie stoi na przeszkodzie, aby administrator […] powierzył IOD prowadzenie, w imieniu administratora […] rejestru czynności przetwarzania danych"[43]. W ocenie Grupy rejestr może być uznany za jedno z narzędzi umożliwiających realizację przez IOD zadań w zakresie monitorowania przestrzegania przepisów przez administratora danych[44].

Podobnie EROD w opublikowanych 27 kwietnia 2023 r. Wytycznych dla małych przedsiębiorstw wprost wskazała, że to IOD prowadzi RCP w takich organizacjach[45]. Skoro zatem w przypadku małych przedsiębiorstw prowadzenie RCP przez IOD nie powoduje konfliktu interesów i jest rozwiązaniem dopuszczalnym, to brak jest powodów, aby twierdzić, że taki konflikt występuje w przypadku innych podmiotów w obrocie gospodarczym. Istnienie konfliktu interesów nie jest bowiem zależne od wielkości podmiotu. Zdaniem EROD IOD może prowadzić zatem RCP w organizacji.

Prawidłowość powyższego stanowiska potwierdzają również wiodące krajowe organy nadzorcze z zakresu ochrony danych osobowych:

a) francuski organ ochrony danych (*Commission nationale de l'informatique et des libertés*), który uznaje, że prowadzenie RCP może być w praktyce zadaniem wykonywanym przez IOD w organizacji administratora[46] [47];

---

[42] E. Bieak – Jomaa, P. Drobek, D. Krajewska-Kekusz M. Młotkiewicz M. Kawecki, T. Soczyńsk, A. Kaczmarek K. Hildebrandt, Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych, Warszawa 2016, str. 59.
[43] Wytyczne (243), str. 20.
[44] Ibidem, str. 20.
[45] EDPB: Guide for small business, dostepne pod adresem: https://edpb.europa.eu/sme-data-protection-guide/data-protection-officer_en (dostęp: 5.04.2024 r.).
[46] Commission nationale de l'informatique et des libertés (CNIL), "Guide on data protection officers", str. 7, dostępny pod adresem URL: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf, (dostęp: 5.04.2024 r.).
[47] Komunikat CNIL "Record of processing activities" z dnia 19.08.2019 r., dostępny pod adresem: https://www.cnil.fr/en/record-processing-activities (dostęp: 5.04.2024 r.).

b) łotewski organ ochrony danych (*Datu valsts inspekcija*), w ocenie którego uzupełnianie i aktualizacja RCP może być bezpośrednim obowiązkiem inspektora, ponieważ nie powoduje konfliktu interesu z pozostałymi zadaniami IOD[48];
c) cypryjski organ ochrony danych (*Επίτροπος Δεδομένων Προσωπικού Χαρακτήρα*), zdaniem, którego, jeżeli w organizacji wyznaczony jest IOD, to inspektor jest właściwą osobą do utworzenia i dalszego uaktualnienia rejestru. Dodatkowo organ ten wskazał w komunikacie na swojej stronie internetowej, że administrator lub podmiot przetwarzający mogą powierzyć IOD zadanie prowadzenia RCP. Jest to bowiem jedno z narzędzi, które pozwala IOD realizować dwa z jego zadań, a mianowicie monitorowanie przestrzegania przepisów oraz informowanie i doradzanie administratorowi lub podmiotowi przetwarzającemu[49];
d) irlandzki organ ochrony danych (*Data Protection Commission*), który za dopuszczalne uznaje kierowanie procesem prowadzenia RCP przez IOD przy wsparciu innych członków personelu administratora[50].

Na zasadność dopuszczalności prowadzenia RCP przez IOD wskazuje się również w opublikowanym na stronie podmiotowej Prezesa UODO dokumencie „Podręcznik Inspektora Ochrony Danych. Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi publicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych". Autorzy powyższego opracowania zauważają, że chociaż prowadzenie RCP jest formalnym obowiązkiem administratora, to w praktyce RCP będzie prowadził IOD[51]. Wskazany powyżej dokument został opracowany w ramach projektu T4DATA, którego celem było podniesienie wiedzy i świadomości w zakresie kompetencji i głównych obowiązków inspektorów ochrony danych. Polski organ właściwy do spraw ochrony danych osobowych we współpracy z organami ochrony danych osobowych z innych państw członkowskich UE brał aktywny udział w projekcie T4DATA od momentu jego inauguracji w 2018 roku, jeszcze jako Generalny Inspektor Ochrony Danych Osobowych.

Należy dodatkowo zauważyć, że RODO nie jest jedynym aktem prawnym w europejskim systemie ochrony danych osobowych, który kreuje wymóg wyznaczenia inspektora ochrony danych oraz określa jego status i zakres wykonywanych przez nich zadań.

Aktem prawnym przewidującym obowiązek powołania IOD dla instytucji i organów Unii Europejskiej jest rozporządzenie 2018/1725, podobnie jak taki obowiązek przewiduje RODO, choć nie każdy administrator lub podmiot przetwarzający ma obowiązek powołania IOD. Oba ww. akty prawne przewidują również obowiązek prowadzenia RCP. Zarówno administrator

[48] Komunikat łotewskiego organu nadzorczego z dnia 19.08.2022 r. "Datu aizsardzības speciālista funkcijas un uzdevumi", dostępny pod adresem: https://www.dvi.gov.lv/lv/jaunums/dviskaidro-DAS_190822 (dostęp: 5.04.2024 r.).
[49] Komunikat na stronie internetowej cypryjskiego organu nadzorczego: Guide to completing the record of processing activities, dostępny pod adresem: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2d_en/page2d_en?opendocument (dostęp: 5.04.2024 r.).
[50] DPC. Guidance Note: Records of Processing Activities (RoPA) under Article 30 GDPR, s. 7, dostępny pod adresem: https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Records%20of%20Processing%20Activities%20%28RoPA%29%20under%20Article%2030%20GDPR.pdf (dostęp: 5.04.2024 r.).
[51] D. Korff, M. Georges, Podręcznik Inspektora Ochrony Danych. Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi publicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych, 2019, str. 136, dostępny pod adresem URL: https://uodo.gov.pl/pl/168/1147 (dostęp: 5.04.2024 r.).

powołujący IOD na podstawie rozporządzenia 2018/1725 ma obowiązek przeciwdziałania występowaniu konfliktom interesów (art. 44 ust. 4 Rozporządzenia 2018/1725) jak i administrator powołujący IOD na podstawie RODO (art. 38 ust. 6 RODO). Uzasadnione jest zatem w ocenie autora opinii, korzystanie z dorobku, który wytworzył się w związku ze stosowaniem ww. aktów prawnych, w zakresie funkcjonowania IOD w organizacji. Z racji tego, że wymogi przewidziane dla inspektorów ochrony danych osobowych w świetle rozporządzenia 2018/1725 pokrywają się w znacznym zakresie z tymi wskazanymi w RODO, to należy uznać, że stanowisko EIOD można *per analogiam* zastosować także w odniesieniu do oceny prawidłowości wykonywania funkcji IOD w świetle przepisów RODO.

Europejski Inspektor Ochrony Danych potwierdził w swoim stanowisku, że jednym z zadań IOD wyznaczonych w instytucjach unijnych (a więc osób powołanych na podstawie analogicznej do RODO regulacji prawnej) jest tworzenie w instytucji RCP[52]. Koresponduje to ze stanowiskiem Komisji Europejskiej, która w komunikacie na swojej stronie internetowej w celu zapewnienia pełnej transparentności Komisji, publikuje swój RCP ze wskazaniem, że to do obowiązków IOD należy prowadzenie tego rejestru[53].

Co istotne, do niedawna polski organ nadzorczy również zdawał się uznawać, że prowadzenia przez IOD RCP nie powoduje konfliktu interesów. W komunikacie z 15 stycznia 2019 opublikowanym na stronie internetowej Urzędu Ochrony Danych Osobowych wprost wskazano, iż „trudno sobie wyobrazić, że inspektor ochrony danych - jako osoba dysponująca odpowiednią wiedzą i umiejętnościami w dziedzinie ochrony danych osobowych - nie będzie angażowała się w tworzenie i prowadzenie rejestrów, a następnie wykorzystywała ich w swojej pracy[54]”. Stanowisko to korespondowało z twierdzeniami zawartymi w publikacji Generalnego Inspektora Ochrony Danych Osobowych[55], w której wskazano na podobieństwa pomiędzy dotychczasowym rejestrem zbiorów danych prowadzonym przez ABI oraz RCP w rozumieniu art. 30 RODO.

Wydaje się jednak, że organ zmienił stanowisko w ww. zakresie, jednak nie wyjaśnił powodów tej decyzji. Zgodnie z treścią wskazaną w jednym z Biuletynów UODO, Dyrektor Departamentu Kontroli i Naruszeń UODO wskazał cyt. „Wiele z naszych zastrzeżeń związanych też było z nałożeniem na inspektorów ochrony danych zadań, które należą do obowiązków administratorów, jak np**.** prowadzenie rejestru czynności przetwarzania, rejestru naruszeń ochrony danych osobowych czy tworzenia wewnętrznych polityk. Inspektor nie może bowiem być obciążony działaniami, które ma oceniać pod kątem ich zgodności z przepisami prawa i regulacjami wewnętrznymi administratora”[56]. W samym Biuletynie UODO wskazano co prawda zastrzeżenie, zgodnie z którym cyt. „Nie wszystkie artykuły i komentarze publikowane w „Biuletynie UODO” stanowią oficjalne stanowisko organu nadzorczego”, jednak ten pogląd znajduje potwierdzenie w komunikacie z 17 stycznia 2024 r., podsumowującym badanie EROD przeprowadzone w ramach CEF, w którym Prezes UODO zasygnalizował, że polski organ

[52] Komunikat EIOD “Data Protection Officer (DPO)”, dostepny pod adresem URL: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (dostęp: 5.04.2024 r.).
[53] Komunikat Komisji Europejskiej, dostępny pod adresem URL https://commission.europa.eu/about-european-commission/service-standards-and-principles/transparency/data-processing-register_en (dostęp: 5.04.2024 r.).
[54] Komunikat Prezesa UODO z 15 stycznia 2019 r.; dostępny pod adresem URL: https://archiwum.uodo.gov.pl/pl/225/659 (dostęp: 5.04.2024 r.).
[55] E. Bielak – Jomaa, P. Drobek, D. Krajewska-Kekusz M. Młotkiewicz M. Kawecki, T. Soczyński, A. Kaczmarek K. Hildebrandt, Wykonywanie obowiązków ABI..., str. 59 i n.
[56] Biuletyn UODO nr 2/04/23, str. 10.

zidentyfikował problemy w zakresie praktyk mogących powodować naruszenie przepisów RODO, „takie jak np.:

> - obciążanie IOD obowiązkami administratora, np. prowadzeniem rejestru czynności przetwarzania”[57].

Prezes UODO dopiero w indywidualnej sprawozdaniu przekazanym w ramach CEF wskazał, w odpowiedzi na pytanie „Czy są jakieś inne problemy lub tematy, które chcieliby Państwo zasygnalizować?” że w jego ocenie Wytyczne w zakresie prowadzenia przez IOD RCP nie są aktualne, ponieważ odnoszą się przez analogię do art. 24^1 lit. d rozporządzenia (WE) 45/2001, które obecnie nie obowiązuje, z uwagi na uchylenie go przez rozporządzenie 2018/1725[58]. Organ nie dostrzega jednak, że zarówno RODO jak i rozporządzenie 2018/1725 stanowiło ewolucję rozwiązań przewidzianych w aktach, które te rozporządzenia zastępowały. Ponadto zarówno EROD jak i EIOD potwierdzają możliwość prowadzenia przez IOD RCP w organizacji na gruncie RODO oraz rozporządzenia 2018/1725, tak jak poprzednio wprost wskazywały na to ww. uchylone już akty prawne. Aktualne zatem pozostają również wskazania sformułowane w Wytycznych przez Grupę Roboczą art. 29. Co więcej, żaden inny krajowy organ nadzorczy nie wskazał w swoim sprawozdaniu krajowym w badaniu CEF na to, że prowadzenie przez IOD RCP jest w jakikolwiek sposób nieprawidłowe. Należy też zwrócić uwagę, że EROD w treści pytania 17 kwestionariusza opracowanego w ramach CEF, zasygnalizował sześć dodatkowych zadań IOD[59], których realizacji może powodować występowanie konfliktu interesów i choć nie jest to z pewnością katalog zamknięty, to prowadzenie RCP lub RCKP nie zostało w tam wskazane.

Zdaniem autora opinii z uwagi na to, że RCKP ma charakter wtórny w stosunku do RCP, dotyczy bowiem procesu przetwarzania danych osobowych opisanego w RCP administratora, to przyjmując, że prowadzenie przez IOD RCP co do zasady nie prowadzi do konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO, to tym bardziej nie zaistnieje on w przypadku prowadzenia RCKP.

Jednocześnie, jak wskazywano wyżej, dla ustalenia, czy realizacja określonego zadania lub obowiązku zleconego dodatkowo IOD jest dopuszczalna, tj. nie powoduje konfliktu interesów, konieczna jest ocena okoliczność realizacji takiego zadania.

Pomimo tego, że co do zasady brak będzie konfliktu interesów w wykonywaniu funkcji IOD, jeżeli to IOD będzie odpowiedzialny za prowadzenie RCP lub RCKP, to mogą występować w praktyce przypadki, w których taki konflikt będzie występował. Może bowiem zdarzyć się, że uzupełnianie RCP lub RCKP nie ma charakteru deklaratoryjnego, a w konkretnej organizacji będzie dokumentem konstytutywnym w tym znaczeniu, że przy jego prowadzeniu i wypełnianiu dochodzi do podejmowania decyzji o celach i sposobach przetwarzania danych osobowych,

---

[57] Komunikat z 17.01.2024 r. Prezesa UODO; dostępny pod adresem URL https://uodo.gov.pl/pl/138/2438 (dostęp: 5.04.2024 r.).

[58] Sprawozdanie Prezesa UODO dostępne pod adresem: https://uodo.gov.pl/pl/138/2960, (dostęp: 5.04.2024 r.).

[59] Raport, str. 25.
Tymi zadaniami są:
1) podejmowanie decyzji w procesie przetwarzania danych osobowych,
2) rozwój procesów przetwarzania danych osobowych prowadzonych w organizacji,
3) przygotowanie i/lub przeprowadzanie oceny skutków dla ochrony danych osobowych,
4) realizowanie praw osób, których dane dotyczą,
5) przygotowanie i/lub negocjowanie umów (np. umów powierzenia przetwarzania danych osobowych),
6) odpowiadanie za zgodne z prawem przestrzeganie przetwarzania danych osobowych.

podstawach prawnych przetwarzania danych osobowych, zakresie danych osobowych przetwarzanych w procesie, czy też o okresach retencji danych.

Jeżeli prowadzenie RCP lub RCKP jest dokumentem, w ramach którego podejmowane są przez IOD decyzje w ww. zakresie, to dochodzić będzie o decydowania o celach i sposobach przetwarzania danych osobowych. Oznacza to tym samym, że IOD prowadząc RCP lub RCKP w tego rodzaju modelu, wykonuje dodatkowe zadania w warunkach konfliktu interesów o charakterze merytorycznym.

Dokumentowanie przez IOD naruszeń zgodnie z art. 33 ust. 5 RODO

Podobnie jak w przypadku RCP oraz RCKP dokumentowanie naruszeń w rozumieniu art. 33 ust. 5 RODO stanowi potwierdzenie istnienia określonych faktów, utrwalenia ich, bez jakiejkolwiek decyzyjności, jeśli chodzi o cele i sposoby przetwarzania danych osobowych.

Samo dokumentowanie zaistniałych naruszeń również, podobnie jak prowadzenie RCP lub RCKP stanowi jednie odwzorowanie i opisanie (zreferowanie) zaistniałego stanu faktycznego. Tego rodzaju dokumentowanie nie zawiera w sobie elementów związanych z decydowaniem o celach i sposobach przetwarzania danych osobowych. Jeżeli jednak w ramach dokumentowania naruszeń, o których mowa w art. 4 pkt 12 RODO, dochodzi do decydowania o zastosowaniu środków naprawczych, zapobiegających wystąpieniu podobnego naruszenia w przyszłości to tego rodzaju dokumentowanie przez IOD naruszeń zaistniałych u administratora będzie prowadziło do konfliktu interesów o charakterze merytorycznym.

Jednocześnie zauważyć trzeba, że prawodawca nie wskazuje formy ani szczegółowych wymogów, którym powinno odpowiadać dokumentowanie zaistniałych naruszeń. W organizacjach spotyka się tabelaryczne ewidencje lub rejestry naruszeń, zawierające zwięzły opis zdarzenia, w tym przyczyny wystąpienia, charakter zdarzenia, stwierdzony poziom ryzyka naruszenia praw i wolności osób, których dotyczyły naruszenie, informację czy dokonano zgłoszenia do organu, czy poinformowano osoby, których dotyczyło zdarzenie oraz chronologię zdarzeń i zastosowane środki mające zapobiec podobnemu zdarzeniu w przyszłości. Nie jest jednak konieczne, aby dokumentowanie naruszeń było prowadzone właśnie w takiej formie.

Zauważyć również trzeba, że prowadzenie ww. ewidencji lub rejestru ma charakter techniczny. Dokonywanie wpisów lub jakichkolwiek innych zmian w rejestrze czy ewidencji naruszeń ma charakter deklaratoryjny i co do zasady nie wiąże się z decydowaniem o celach oraz sposobach przetwarzania danych, w tym podejmowaniem działań naprawczych przez administratora w związku ze stwierdzonym naruszeniem.

Takie stanowisko potwierdzają przyjęte przez EROD Wytyczne 09/2022, w których EROD wyjaśniając rolę IOD w procesie zgłaszania naruszeń wskazał, że administrator może powierzyć inspektorowi prowadzenie takiego rejestru w swoim imieniu. W tym miejscu należy także zauważyć, że Wytyczne (250), które zostały zastąpione przez wskazane powyżej Wytyczne 09/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych zgodnie z RODO, w rozdziale poświęconym prowadzeniu rejestrów naruszeń ochrony danych również wskazywały, że „Inspektor ochrony danych może również otrzymać dodatkowe zadanie polegające na prowadzeniu takich rejestrów” (rozdział V pkt B powołanych wytycznych). Utrzymanie stanowiska Grupy Roboczej Art. 29 przez EROD w Wytycznych 09/2022 dodatkowo potwierdza dopuszczalność prowadzenia rejestru naruszeń przez IOD w świetle przepisów RODO.

Należy w tym miejscu zaznaczyć, że potwierdzanie stanu faktycznego, bez kompetencji do ingerencji w proces przetwarzania danych osobowych jest cechą wspólną zarówno dokumentacji dotyczącej naruszeń jak i RCP.

Podkreślić trzeba, że również w publikacji Generalnego Inspektora Ochrony Danych Osobowych z 2016 r. wprost wskazano cyt. „zgodnie z art. 33 ust. 5 RODO, administrator dokumentuje wszelkie naruszenia ochrony danych osobowych", jednak „wymóg stworzenia oraz aktualizowania takiej dokumentacji ciążył będzie na inspektorze ochrony danych jako na osobie posiadającej największą wiedzę o wszelkich zdarzeniach mogących rodzić ryzyko naruszenia zasad ochrony danych."[60].

Potencjalnie możliwe jest jednak, żeby dokumentowanie naruszenia stanowiło konflikt interesów w wykonywaniu funkcji IOD. Zadanie jednak musiałoby być realizowane w taki sposób, że z chwilą dokumentowania naruszenia IOD decyduje o zastosowaniu środków zaradczych, mających na celu zapobiegnięcie podobnym zdarzeniom w przyszłości lub mających zapobiec negatywnym skutkom dla praw i wolności osób, których dotyczyło naruszenie. Takie działanie miałoby bowiem wpływ na decydowanie o celach i sposobach przetwarzania danych osobowych.

Udział IOD w ocenie skutków dla ochrony danych osobowych

Prawodawca w art. 35 ust. 2 RODO nie określa zakresu zaangażowania IOD w dokonywanie oceny skutków dla ochrony danych osobowych, wskazując jedynie, że administrator powinien skonsultować się w jej ramach z IOD.

Zgodnie z art. 35 ust. 7 RODO opracowanie kompletnej DPIA obejmuje co najmniej:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
2) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Oznacza to, że przeprowadzenie DPIA może obejmować zarówno aspekt określenia celu przetwarzania, jego modyfikacji lub ingerencji w planowany proces przetwarzania, w tym ocenę niezbędności i zasadności planowanego procesu (pkt 1 i 2) jak i aspekt sposobu przetwarzania, odnoszący się do wskazania środków, których podjęcie jest planowane w celu mitygowania ryzyka (pkt 4).

[60] E. Bieak – Jomaa, P. Drobek, D. Krajewska-Kekusz, M. Młotkiewicz, M. Kawecki, T. Soczyński, A. Kaczmarek K. Hildebrandt..., str. 59.

Jeżeli zatem przekazanie do realizacji lub zlecenie przygotowania DPIA inspektorowi ochrony danych polegałoby na konieczności podjęcia przez IOD decyzji, co do dopasowania środków bezpieczeństwa w celu zaradzenia ryzyku, jakie wiąże się z planowanym procesem przetwarzania, środków zmierzających do wyważenia interesów administratora z interesami podmiotów danych oraz dookreślenia celu przetwarzania – to takie działania będą stanowiły o występowaniu konfliktu interesów o charakterze merytorycznym. Dodatkowo, jeżeli IOD będzie podejmował działania w obszarze decydowania o celach i sposobach przetwarzania, co do planowanego procesu przetwarzania danych osobowych, to może taka aktywność również spowodować konflikt interesów.

Jeżeli jednak rola IOD ograniczona byłaby, poza doradzaniem administratorowi w ramach DPIA, do czynności techniczny polegających na np. uzupełnieniu formularza lub opracowaniu metodologii DPIA, to takie działania nie powinny powodować powstania konfliktu interesów.

Udział IOD w tworzeniu dokumentów wewnętrznych dotyczących ochrony danych osobowych w organizacji

Częstym zjawiskiem jest, że organizacja wyznacza IOD jako osobę dedykowaną do zajmowania się całościowo obszarem ochrony danych osobowych. Jest to bowiem osoba wyspecjalizowana w ww. tematyce i posiada największe kwalifikacje w tym zakresie. Co więcej, doświadczony IOD będzie posiadał wiedzę jakie rozwiązania najczęściej sprawdzają się w organizacji.

Z uwagi na powyższe niektórzy administratorzy (podmioty przetwarzające) mając na uwadze fachowość IOD zlecają mu dodatkowo sprawowanie nadzoru nad przetwarzaniem danych osobowych, w tym opracowanie i wdrożenie rozwiązań, które mają zapewnić zgodność organizacji z przepisami o ochronie danych osobowych.

Jak wskazywano wyżej, IOD nie może być odpowiedzialny za opracowanie i wdrożenie rozwiązań z zakresu ochrony danych osobowych w organizacji. Nie oznacza to jednak, że IOD nie może brać udziału w tworzeniu ww. dokumentacji i procedur wewnętrznych związanych m. in. z zabezpieczaniem danych osobowych, zarządzaniem naruszeniami przez IOD, obsługą wniosków podmiotów danych osobowych. Żeby jednak proaktywny udział IOD był możliwy, tj. polegający nie tylko na wskazywaniu niedoskonałości procedury lub dokumentu, ale również na przedstawieniu propozycji zmian konieczne jest ustalenie takich zasad prac nad ww. dokumentami, by zapewnić niezależność i obiektywizm wykonywania zadań IOD przewidzianych w art. 39 ust. 1 RODO.

W doktrynie wskazuje się przy tym, że obowiązki inspektora ochrony danych w zakresie monitorowania obejmują również organizację ochrony danych, tak więc jest to szczególny przypadek napięcia między konsultacją a monitorowaniem. Charakteryzuje się on daleko idącym wpływem organizacji ochrony danych na wszystkie systemy i przetwarzanie danych w organizacji. Struktura organizacji ochrony danych wymaga wysokiego stopnia kreatywności w celu wdrożenia wymogów prawnych w praktyce przetwarzania danych. Ustanowienie organizacji ochrony danych wiąże się z podejmowaniem niezależnych decyzji koncepcyjnych przez inspektora ochrony danych. Może to choć nie musi wykraczać poza stopień niezależności przypisywany inspektorowi ochrony danych. Jeżeli inspektor ochrony danych przekroczy ten stopień niezależności przy tworzeniu organizacji ochrony danych, zwykłe

napięcie między doradztwem a monitorowaniem może przekształcić się w konflikt interesów[61]. Potwierdza to zatem, że rola IOD, również w obszarze tworzenia dokumentacji wewnętrznej administratora może mieć aktywny charakter, choć konieczna jest przy tym ostrożność, aby zaangażowanie IOD nie wiązało się z występowaniem konfliktu interesów.

Przede wszystkim proces tworzenia dokumentacji wewnętrznej nie powinien zakładać, że o ostatecznym kształcie procedur i zaprojektowanych rozwiązań decyduje IOD. Opracowanie procedur wewnętrznych z obszaru ochrony danych osobowych nie może również ograniczać się wyłącznie do zatwierdzenia jej przez administratora; przy takim bowiem założeniu to faktycznie IOD będzie decydował o sposobach przetwarzania danych osobowych w organizacji. Z perspektywy badania występowania konfliktu interesów w organizacji istotne jest bowiem rzeczywiste, a nie formalne występowanie takiego konfliktu.

Możliwe jest zatem opracowanie przez IOD wzorcowej dokumentacji dotyczącej ochrony danych osobowych, która następnie zostaje dostosowana do organizacji (odpowiednio zmodyfikowana) i wdrożona przez inną osobę w organizacji niż IOD. Również niewykluczone jest opracowanie wstępnego projektu dokumentów przez IOD, które następnie będą podlegały dalszym pracom dostosowawczym. Istotny jest bowiem poziom zaangażowania IOD w opracowywanie ostatecznego kształtu procedur i dokumentacji administratora, jak również ustalenie czy elementy, na które IOD miał bezpośredni wpływ, mają znaczenie z perspektywy decydowania o celach i sposobach przetwarzania danych osobowych.

Potencjalnie, po otrzymaniu propozycji dokumentu lub procedury, poddanie jej ocenie, w zależności od rodzaju administratora, działowi prawnemu lub technicznemu, które traktując opracowaną przez IOD jako podstawę do dalszych działań, dostosują zgodnie z potrzebami organizacji i ją wdrożą, nie będzie powodowało decyzyjnej roli IOD w procesie.

Nie jest to rozwiązanie uniwersalne i jego skuteczność zależeć będzie od okoliczności faktycznych jak i kultury organizacyjnej administratora, ponieważ jak wskazano wyżej, o istnieniu konfliktu interesów decydują każdorazowo okoliczności faktyczne u konkretnego administratora (podmiotu przetwarzającego). Nie można przyjąć *a priori,* bez zapoznania się z konkretnymi, całościowymi okolicznościami stanu faktycznego, że w ramach realizacji określonego zadania będzie lub nie będzie dochodziło do konfliktu interesów IOD.

Chociaż IOD nie powinien być odpowiedzialny za wdrożenie określonego rozwiązania u administratora, jak również to nie on faktycznie powinien decydować o jego wyborze, to mając na uwadze art. 38 ust. 1 RODO, powinien on być włączany w proces jego opracowania.

W praktyce spotykane jest również rozwiązanie, polegające na zlecaniu IOD załatwiania spraw, w tym składania oświadczeń, w odpowiedzi na wnioski podmiotów danych, z zakresu realizacji praw przewidzianych w rozdziale III RODO[62]. Jednak w ocenie autora opinii nie jest to działanie prawidłowe, właśnie ze względu na konflikt interesów.

Nawet jeżeli treść korespondencji zostaje faktycznie opracowana przez pracownika administratora, to IOD, składa oświadczenie w piśmie skierowanym do podmiotu danych, czym potwierdza i akceptuje ostateczne brzmienie treści odpowiedzi. W tym przypadku złożenie podpisu nie jest bowiem tylko czynnością techniczną, a stanowi oświadczenie woli i w tym kontekście element reprezentowania administratora, co jest jednoznaczne z podejmowaniem

[61] P.Grosmann, Die Interessenkonflikte der betrieblichen...,str. 124
[62] Ibidem,str. 110

w jego imieniu oraz na jego rzecz czynności dotyczącej decydowania o realizacji prawa podmiotu danych osobowych.

Jeżeli jednak rola IOD ograniczona zostałaby w tym procesie jedynie do czynności technicznej, tj. przesłania korespondencji opatrzonej podpisem innej osoby niż IOD, to takiego działania nie można zakwalifikować jako konflikt interesów w wykonywaniu funkcji IOD.

Podejmowanie wyłącznie czynności technicznych nie powoduje ryzyka konfliktu interesów w wykonywaniu funkcji IOD, nie stanowi bowiem ingerencji w niezależność, obiektywizm i skuteczność wykonywania zadań wymienionych w art. 39 ust. 1 RODO.

Tak rozumiana rola IOD w żadnych stopniu nie narusza jego zadania określonego w art. 38 ust. 4 RODO jako tzw. punktu kontaktowego dla osoby, której dane dotyczą. IOD przyjmuje wszelkie kierowane do niego przez podmioty danych wiadomości, a także może komunikować się z tymi osobami we wszystkich sprawach związanych z wykonywaniem praw przysługujących im na mocy RODO (np. roboczo informując o zakresie i sposobie realizacji tych praw), jak również może zajmować się – co wspomniano powyżej – technicznym przesyłaniem odpowiedzi administratora załatwiającej wniosek.

Podobnie należy ocenić sytuację, w której IOD opatruje swoim podpisem zgłoszenie naruszenia w rozumieniu art. 33 ust. 1 RODO kierowane do organu nadzorczego. Takie działanie będzie wskazywać na istnienie konfliktu interesów o charakterze merytorycznym[63], będzie bowiem wiązać się z reprezentowaniem administratora, potwierdzeniem ostatecznego brzmienia treści zgłoszenia, zastosowanych środków w reakcji na naruszenie oraz ewentualnej propozycji zawiadomienia osoby, której dotyczyło naruszenie (art. 34 RODO).

W ocenie autora opinii **dopuszczalne jest proponowanie przez IOD określonego brzmienia dokumentacji wewnętrznej administratora**, dopóki taka propozycja nie będzie oznaczać rzeczywistego decydowania o celach i sposobach przetwarzania danych osobowych.

Ponadto, jeżeli opracowanie dokumentacji wewnętrznej przez IOD polegać ma wyłącznie na potwierdzeniu jedynie obecnych procesów przetwarzania danych oraz przepływu informacji wewnątrz organizacji, a następnie na sygnalizacji administratorowi obszarów potrzebnych zmian ze wskazaniem potencjalnych rozwiązań zauważonych nieprawidłowości, to takie działanie nie będzie powodować występowania konfliktu interesów. Będzie to bowiem faktycznie czynność dokumentacyjna, nieposiadająca charakteru merytorycznego (w obszarze potwierdzenia stanu faktycznego); natomiast sformułowanie zaleceń (doradzanie) zostanie zrealizowane w ramach zadań IOD (art. 39 ust. 1 lit. a RODO).

Wszelkie zadania polegające na dokumentowaniu zdarzeń lub utrwalaniu (raportowaniu) stanu rzeczywistego w organizacji nie powinny zostać uznane za powodujące ryzyko występowania konfliktu interesów w rozumieniu art. 38 ust. 6 RODO.

Pełnienie roli pełnomocnika administratora (podmiotu przetwarzającego)

Zdarza się również, że administrator (podmiot przetwarzający) zleca IOD reprezentowanie go w toku postępowań administracyjnych prowadzonych przez Prezesa UODO lub w postępowaniu sądowo-administracyjnym w zakresie kontroli Prezesa UODO w sprawach indywidualnych.

[63] Ibidem, str.110.

Zauważyć trzeba, że Grupa Robocza Art. 29 sygnalizuje potencjalny konflikt interesów w przypadku, gdy cyt. „**zewnętrzny IOD** zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych.”[64].

Występowanie przez IOD w roli pełnomocnika wiązać się będzie potencjalnie z decydowaniem o celach i sposobach przetwarzania danych osobowych, w zakresie przekazywania danych osobowych uczestnikom postępowania prowadzonego przed sądem powszechnym lub organowi nadzorczemu. Pełnomocnik w postępowaniu sądowym lub administracyjnym powinien działać na korzyść swojego mocodawcy – co może oznaczać, że IOD reprezentując mocodawcę będzie albo przywoływał fakty i okoliczności świadczące na niekorzyść administratora (np. fakt niezastosowania rekomendacji IOD), albo wbrew negatywnej ocenie jakiegoś rozwiązania, przedstawiał wyłącznie argumenty przemawiające za jego prawidłowością. Innymi słowy pełnienie roli pełnomocnika administratora przez IOD może doprowadzić do sprzecznych twierdzeń IOD, co do tej samej okoliczności istniejącej u administratora.

Celem działalności IOD pozostaje niezależne zapewnienie przestrzegania przepisów o ochronie danych osobowych oraz polityk ochrony danych, a tymczasem pełnomocnik w postępowaniu dąży do osiągnięcia dla swojego mocodawcy określonych celów procesowych. Oprócz tego pełnomocnik zasadniczo działa zgodnie z instrukcjami swojego mocodawcy, natomiast IOD w swojej działalności merytorycznej ma pozostawać wolny od wpływu administratora.

Oznacza to, że IOD nie powinien być również wskazywany jako pełnomocnik w toku postępowania (administracyjnego lub sądowego), w którym udział bierze administrator (podmiot przetwarzający). Rola pełnomocnika wiązać się będzie m. in. z decydowaniem o zakresie i celu przekazania danych osobowych innemu podmiotowi.

IOD nie powinien również reprezentować administratora lub podmiotu przetwarzającego w ramach negocjowania umów, których przedmiotem jest przetwarzanie danych osobowych, lub umów powierzenia przetwarzania danych osobowych[65]. Umocowanie IOD i reprezentowanie administratora (podmiotu przetwarzającego) w ramach negocjowania umowy jest związane z faktycznym decydowaniem o treści postanowień umowy. W ramach negocjowania umowy dochodzi bowiem do ustalenia jej brzmienia, wzajemnych praw i obowiązków stron, w tym w obszarze ochrony danych osobowych. Oznacza to, że IOD *de facto* odpowiadałby za określenie sposobów przetwarzania danych osobowych i ich celów, co następnie podlegałoby jego weryfikacji w związku z wykonywaniem zadań podstawowych IOD – co naruszać będzie obiektywizm wykonywania funkcji IOD[66].

Z tej samej przyczyny konflikt interesów występował będzie, jeżeli administrator udzieli upoważnienia IOD do wydawania w jego imieniu upoważnień do przetwarzania danych osobowych w rozumieniu art. 29 RODO. Oznaczać to będzie bowiem faktyczne decydowanie przez IOD o tym, jakie osoby w organizacji są uprawnione do dostępu do danych - co wskazuje, że w ramach organizacji decyzja o sposobach przetwarzania danych osobowych podejmowana jest przez IOD.

---

[64] Wytyczne (243), str. 17.

[65] Komunikat Prezesa UODO z 10.05.2022 r. dostępny pod adresem URL:https://archiwum.uodo.gov.pl/pl/225/2374 (dostęp: 5.04.2024 r.)

[66] Raport EROD, str. 25-26.

Kierowanie pracami zespołu IOD oraz korzystanie z zasobów administratora

Jak wskazano przy okazji omawiania konfliktu interesów o charakterze czasowym IOD może być wspierany w wykonywaniu swoich zadań przez wyznaczony do tego zespół osób. Nie jest to zadanie opisane w art. 39 ust. 1 RODO, należy więc uznać, że stanowi ono zadanie dodatkowe IOD, w rozumieniu art. 38 ust. 6 RODO.

IOD powinien aktywnie koordynować pracę tego zespołu, biorąc w niej bezpośredni udział i podejmując decyzje co do kierunków prac; jednak wiązać się do będzie z działaniami, które będą miały związek z ochroną danych osobowych w organizacji, a nawet z operacjami na danych osobowych.

W przypadku IOD będącego członkiem personelu administratora (podmiotu przetwarzającego), IOD korzysta w większy lub mniejszym stopniu z zasobów i narzędzi zapewnionych przez administratora (podmiot przetwarzający). Będzie on również stosował się do przewidzianych przez administratora procedur w tym związanych bezpośrednio z ochroną danych osobowych. IOD w ramach swojej pracy komunikuje się z pracownikami w organizacji oraz podmiotami współpracującymi, a zatem w codziennej pracy będzie też kierował korespondencję wewnętrzną lub zewnętrzną za pomocą skrzynki elektronicznej zapewnionej mu w organizacji, będzie prowadził notatki i opracowywał pisma wewnętrzne, listy pracowników, którzy wzięli udział w prowadzonych szkoleniach, prowadził i przechowywał dokumentację, w tym zawierającą dane osobowe.

Przyjmując zatem założenie, że konflikt interesów w rozumieniu art. 38 ust. 6 RODO występuje z samego tylko powodu, że to IOD bierze udział w procesie konstruowania jakiegoś dokumentu lub dokumentuje zdarzenie, które potem podlegać ma monitorowaniu przez IOD, to IOD nie mógłby korzystać z jakiegokolwiek narzędzia zapewnianego przez administratora. Nie mógłby również współpracować ze swoim zespołem, tworzyć notatek czy list, skoro te czynności, prowadzone w ramach organizacji administratora, również będą podlegały monitorowaniu przez IOD.

Zauważyć trzeba, że IOD będzie uczestniczył w wewnętrznych procesach przetwarzania danych osobowych, które następnie będą podlegały jego monitoringowi. Co więcej, potencjalnie możliwe jest, że w wyniku działania IOD lub członka zespołu IOD dojdzie do naruszenia w rozumieniu art. 4 pkt 12 RODO, które będzie wymagało dokonania stosownego zgłoszenia do Prezesa UODO oraz poinformowania podmiotu danych.

Przyjmując, że IOD nie może wykonywać jakichkolwiek czynności, które następnie podlegałyby monitorowaniu prowadziłoby do sytuacji, w której nie może on wykonać jakichkolwiek czynność w organizacji, które wiązałyby się choćby z przechowywaniem danych osobowych. Korzystanie z narzędzi i zasobów służących do wykonywania zadań IOD nie może zatem powodować występowania konfliktu interesów IOD.

Jednakże w ocenie autora opinii nie dochodzi w takim przypadku do naruszenia niezależności, obiektywizmu i skuteczności wykonywania zadań IOD, opisanych w art. 39 ust. 1 RODO.

Czynności wykonywane w ramach funkcjonowania IOD w organizacji mają charakter techniczny i są związane ze sposobem wykonywania zadań przez IOD, choć mogą stanowić procesy i operacje również związane z danymi osobowymi. Należy pamiętać, że celem regulacji art. 38 ust 6 RODO, jest zapewnienie IOD możliwości wykonywania swoich zadań określonych w art. 39 ust. 1 RODO. Nawet zatem jeżeli IOD weryfikowałby operacje dot.

danych osobowych w ramach zespołu, którym kieruje IOD, lub w ramach samych czynności niezbędnych w pracy IOD (np. wysyłanie i przechowywanie wiadomości mailowych), w celu wykonywania zadań IOD, to nie można stwierdzić, że dochodzi do uchybienia w obszarze prawidłowości wykonywania zadań IOD, w tym obiektywizmu i niezależności. IOD nie podejmuje bowiem decyzji o celach i sposobach przetwarzania danych osobowych w ramach zespołu IOD, czy też własnych czynności wewnątrz organizacji, zastępując w tej roli administratora.

Część IV. Wpływ formy wykonywania funkcji IOD (wewnętrzny oraz outsourcing) na konflikt interesów oraz jego unikanie

Wykonywanie funkcji IOD odbywać się może w dwóch podstawowych formach – wewnętrzna oraz outsourcingu. Zgodnie z pierwszą z nich IOD jest członkiem personelu administratora i działając na podstawie umowy o pracę lub umowy cywilnoprawnej, korzysta w całości albo w części z zasobów administratora w celu wykonywania swoich zadań i sprawuje swoją funkcję tylko w tym podmiocie. Zgodnie z drugą z nich administrator korzysta z usług podmiotu zewnętrznego, który albo samodzielnie wykonuje funkcję IOD albo zapewnia wykonywanie funkcji IOD przez pracownika podmiotu zewnętrznego. W takim przypadku podmioty wskazują zwykle w treści umowy kto będzie wykonywał funkcje IOD w podmiocie i ta osoba zostaje zgłoszona przez administratora (podmiot przetwarzający) do Prezesa UODO w wykonaniu obowiązku art. 10 Ustawy z 2018 r.

Każda z tych form wiąże się z innymi ryzykami występowania konfliktu interesów w wykonywaniu funkcji IOD.

Outsourcing funkcji IOD

W przypadku outsourcingu funkcji IOD co do zasady nie powinien występować konflikt interesów o charakterze ustrojowym w podmiocie, w którym funkcja ta będzie wykonywana.

Brak jest bowiem w takim sytuacji poległości służbowej u administratora (podmiotu przetwarzającego), z uwagi na to, że IOD nie należy do struktury organizacyjnej tego podmiotu. W ramach outsourcingu IOD zlecane są zadania wykraczającego poza katalog określony w art. 39 ust. 1 RODO, jednak zwykle są one związane z ochroną danych osobowych, jak np. prowadzenie RCP czy dokumentowanie zaistniałych naruszeń w organizacji.

Przy realizacji takich zadań IOD odpowiada w ramach wykonywanej umowy jako jej strona przed administratorem (podmiotem przetwarzającym) lub bezpośrednio przed najwyższym kierownictwem podmiotu, który zawarł umowę z administratorem (podmiotem przetwarzającym). Jednocześnie wykonywanie funkcji IOD w ramach outsourcingu nie oznacza, że obowiązek podległości IOD najwyższemu kierownictwu administratora (podmiotowi przetwarzającego) jest wyłączony, jednak dotyczy on wtedy (w przypadku braku podległości organizacyjnej i porządkowej IOD) możliwości dostępu do najwyższego kierownictwa przez IOD w celu rozliczenia się z wykonywania swoich zadań oraz m. in. doradzania i informowania administratora w przedmiocie ochrony danych osobowych w organizacji[67].

W zakresie konfliktu interesów o charakterze merytorycznym w przypadku outsourcingu funkcji IOD trzeba wskazać, że jeżeli strony nie przewidzą inaczej w umowie pomiędzy podmiotami,

[67] Wytyczne (243), str. 16.

administratorowi (podmiotowi przetwarzającemu) nie przysługują uprawnienia w zakresie karania lub nagradzania IOD, jak i nie są oni władni do wydawania IOD jakichkolwiek instrukcji w obszarze wykonywania zadań przez IOD. Jak podkreśla się w literaturze, jedną z korzyści niezależnego zewnętrznego inspektora ochrony danych jest domyślna niezależność od instrukcji wydawanych IOD przez jakąkolwiek osobę z organizacji[68].

Podmioty świadczące usługę outsourcingu funkcji IOD nie ograniczają się zwykle do świadczenia tej usługi na rzecz jednego tylko podmiotu. Oznacza to, że konflikt interesów o charakterze merytorycznym może zaistnieć również w przypadku, gdy ten sam IOD będzie wykonywał swoją funkcję jednocześnie w dwóch podmiotach pozostających ze sobą w relacji prawnej. Taki konflikt może powstać, gdy pomiędzy dwoma podmiotami będzie dochodziło do udostępniania sobie danych osobowych lub powierzania wykonywania określonych operacji na danych.

O ile zgodnie z art. 38 ust. 6 RODO obowiązek unikania konfliktu interesów spoczywa na administratorze (podmiocie przetwarzającym) to należy zwrócić uwagę, że podmioty te nie mają narzędzi umożliwiających pozyskanie informacji o występowaniu ww. konfliktu interesów. W ocenie autora opinii IOD jako podmiot profesjonalny powinien informować administratora (podmiot przetwarzający) o ewentualnych przeszkodach w pełnieniu swojej funkcji, w tym o możliwym występowaniu konfliktu interesów, który uniemożliwiał będzie prawidłowe wykonywanie funkcji IOD.

Pełnienie funkcji IOD w wielu podmiotach może oznaczać również występowanie po stronie IOD konfliktu interesów o charakterze czasowym.

Ponownie wskazać trzeba, że prawodawca nie przewiduje ograniczeń co do liczby i wielkości podmiotów, w których IOD może pełnić swoją funkcję. Jak już wyjaśniono wykonywanie funkcji IOD nie musi polegać na samodzielnym wykonywaniu określonych czynności technicznych w organizacji. Wystarczający jest bowiem nadzór i ostateczne decydowanie przez IOD o kształcie np. rekomendacji, informacji, zaleceń, których adresatem ma być administrator (podmiot przetwarzający)[69].

Rola IOD nie może jednak ograniczyć się do wskazania jedynie tej osoby w zgłoszeniu do Prezesa UODO w trybie art. 10 Ustawy z 2018 r. Nadzór sprawowany przez IOD, o którym mowa powyżej, powinien mieć rzeczywisty charakter.

Oznacza to tym samym, że IOD powinien aktywnie weryfikować i koordynować prace członków zespołu, którzy bezpośrednio kontaktują się z administratorami (podmiotami przetwarzającymi) będącymi zleceniodawcami usługi outsourcingu funkcji IOD.

Istotne jest zagwarantowanie rzeczywistego udziału IOD w obsłudze klientów, na co wskazywać może nie tylko bezpośredni dowód na taki udział (np. wiadomości mailowe) ale również np. zasady obsługi klientów podmiotu zapewniającego usługę outsourcingu IOD.

Jeżeli doszłoby do ryzyka konfliktu czasowego IOD jako realizujący usługę, powinien w ramach otrzymywanego wynagrodzenia zwiększyć zasoby osobowe do obsługi IOD, dokonać wewnętrznych modyfikacji zasad obsługi klientów, a w ostateczności – zrezygnować z pełnienia funkcji IOD, z uwagi na brak możliwości rzeczywistego jej wykonywania, pomimo

[68] P. Grosmann, Die Interessenkonflikte der betrieblichen..., str. 61-62
[69] Wytyczne (243), str. 15.

zapewnienia sobie odpowiednich zasobów osobowych w ramach zawartej umowy z administratorem (podmiotem przetwarzającym).

W przypadku pełnienia funkcji IOD w ramach umowy z podmiotem zewnętrznym istotnym narzędziem dla unikania konfliktu interesów o charakterze ustrojowym i merytorycznym jest, co oczywiste, doprecyzowanie praw i obowiązków stron, ale również określenie praw i obowiązków IOD oraz jakie ewentualne uprawnienia i zadania posiadają w stosunku do siebie IOD i administrator (podmiot przetwarzający). Dla unikania konfliktu interesów o charakterze czasowym istotne znaczenie ma z jednej strony samoświadomość IOD co do możliwości rzeczywistego pełnienia funkcji w wielu podmiotach jednocześnie oraz określenie poziomu zaangażowania IOD w wykonywanie zadań określonych w umowie pomiędzy zleceniodawcą i zleceniobiorca usługi outsourcingu funkcji IOD.

Pełnienie funkcji IOD jako członek personelu administratora (podmiotu przetwarzającego)

IOD będąc członkiem personelu administratora (podmiotu przetwarzającego) podlega odpowiedzialności organizacyjnej i porządkowej, co oznacza, że jego status powinien wynikać z dokumentacji wewnętrznej zarówno w tym celu, by pozostali członkowie organizacji mieli świadomość tego statusu, jak i w celu zagwarantowania niezależności IOD, w tym uniknięcia potencjalnych sytuacji mogących powodować powstanie konfliktu interesów.

Podległość IOD najwyższemu kierownictwu w zakresie dodatkowych obowiązków i zadań IOD wynikających wprost z art. 39 ust. 1 RODO powinna zostać zagwarantowana w dokumentacji wewnętrznej administratora, co umożliwi wykazanie braku ryzyka występowania konfliktu interesów o charakterze ustrojowym.

Należy jednak przy tym pamiętać, że decydujące znaczenie ma, czy IOD rzeczywiście podlega wyłącznie najwyższemu kierownictwu w organizacji – samo jedynie formalne, nieodpowiadające rzeczywistości określenie pozycji IOD w ww. sposób nie będzie oznaczało, że nie dochodzi do konfliktu interesów o charakterze ustrojowym.

Wykonywanie funkcji IOD w ramach organizacji administratora jest związane również z podległością służbową pracownika. Oznacza to, że potencjalnie istnieje ryzyko wydawania IOD instrukcji przez najwyższe kierownictwo, w zakresie wykonywania przez niego zadań określonych w art. 39 ust. 1 RODO.

W celu uniknięcia występowania ww. konfliktu możliwe jest określenie w dokumentacji wewnętrznej administratora (podmiotu przetwarzającego) sytuacji i obszarów, w których IOD może otrzymywać polecenia oraz te, które mieszczą się w autonomii IOD. Stworzenie takiego dokumentu nie jest obowiązkiem przewidzianym w prawie, choć może być pomocne w celu wykazania braku wydawania tego rodzaju instrukcji IOD. Nie uzasadnionym jednak byłoby przyjęcie, że w przypadku braku ww. dokumentu w organizacji występuje konflikt interesów. Dopiero wydanie takiej instrukcji IOD oraz brak odpowiedniej reakcji na takie zdarzenie może bowiem powodować wystąpienie konfliktu interesów. Jednocześnie IOD powinien poinformować najwyższe kierownictwo, jeżeli wydane mu instrukcje dotyczą obszaru, w którym nie powinien on ich otrzymywać.

Elementem konfliktu interesów o charakterze merytorycznym jest decydowanie o celach i sposobach przetwarzania danych osobowych, co w przypadku, gdy IOD jest członkiem personelu administratora, może wiązać się z zajmowaniem przez niego w organizacji

dodatkowej funkcji, w ramach której dochodzi do decydowania o celach i sposobach przetwarzania danych.

Zajmowanie stanowiska kierowniczego najczęściej związane jest z decydowaniem o celach i sposobach przetwarzania danych osobowych; osoba kierująca działem, departamentem lub samym podmiotem (np. członek zarządu) posiada zakres autonomii decyzyjnej również w zakresie podejmowania czynności w imieniu administratora na zewnątrz. Grupa Robocza Art. 29 wskazuje w Wytycznych (243), że zajmowanie przez IOD stanowiska dyrektora generalnego, dyrektora ds. operacyjnych, dyrektora finansowego, dyrektora ds. medycznych, kierownika działu marketingu, kierownika działu HR, kierownika działu IT będzie wiązać się najprawdopodobniej z konfliktem interesów w rozumieniu art. 38 ust. 6 RODO[70]. Grupa Robocza Art. 29 podkreśla jednak, że decydujące dla ustalenia, czy dojdzie do konfliktu interesów jest decydowanie o celach i sposobach przetwarzania danych osobowych, a nie sam fakt zajmowania określonego stanowiska w organizacji.

Organy nadzorcze w państwach członkowskich Unii Europejskiej identyfikują również jako mogące powodować występowanie konfliktu interesów, zajmowanie stanowiska kierownika departamentu zarządzana ryzykiem oraz specjalnej jednostki dochodzeniowej, kierownik działu zgodności[71] i przeciwdziałania praniu pieniędzy[72], dyrektor compliance[73], dyrektor departamentu audytu wewnętrznego, zarządzania ryzykiem i zgodności[74].

W doktrynie sygnalizuje się jednocześnie, że wyznacznikiem, czy IOD może zajmować inne stanowisko w organizacji (z perspektywy występowania konfliktu interesów o charakterze merytorycznym) jest ustalenie, czy ze stanowiskiem tym związane są kompetencje decyzyjne w zakresie przetwarzania danych[75]. Wskazuje się nawet, że uprawnienia pracownika do administrowania małymi podobszarami systemów przetwarzania danych nie są jeszcze w stanie stanowić podstawy do stwierdzenia konfliktu interesów[76].

Konieczne jest zatem ustalenie, czy IOD w zakresie dodatkowego zadania nie będzie decydować o celach i sposobach przetwarzania danych osobowych.

W przypadku konfliktu interesów o charakterze czasowym konieczna jest analiza większego zakresu okoliczności, niż ma to miejsce w przypadku realizowania funkcji IOD w ramach outsourcingu. Pracodawca powinien zatem ustalić czy wymiar czasu pracy jest wystarczający na wykonywanie zadań IOD, biorąc pod uwagę wielkość organizacji, poziom skomplikowania procesów przetwarzania, skalę przetwarzania danych osobowych oraz sytuację, w której znajduje się podmiot pod kątem ochrony danych osobowych – co może stwierdzić również IOD w ramach wstępnego sprawdzenia standardów organizacji.

Możliwe jest zatem zwiększenie czasu pracy IOD (jeżeli wcześniej wykonywał zadania IOD w niepełnym wymiarze godzin), zlecenie wykonywanie dodatkowych zadań, które do tej pory wykonywał IOD innej osobie w organizacji, lub zapewnienie IOD wsparcia osobowego, w postaci jednej lub większej liczby osób, które powinny wesprzeć IOD w wykonywaniu jego

[70] Wytyczne (243), str. 17.
[71] Decyzja APD (Belgia) z dnia 16 grudnia 2021 r., nr 141/2021.
[72] Decyzja CNPD (Luksemburg) z dnia 13 października 2021 r., 36FR/2021.
[73] Decyzja APD (Belgia) z dnia 13 października 2021 r., nr 37FR 2021,
[74] Decyzja APD (Belgia) z dnia 28 maja 2020 r., nr 18/2020,
[75] P.Grosmann, Die Interessenkonflikte der betrieblichen..., str. 45 – 46.
[76] Ibidem, str. 45 – 46.

zadań. To IOD jednak powinien decydować o ostatecznym kształcie realizowanych zadań, w tym brzmieniu rekomendacji przedstawianych administratorowi.

V. Możliwe modele pełnienia funkcji IOD

Analiza regulacji dotyczących IOD, jak również stanowisk EROD i Grupy Roboczej Art. 29 prowadzi do wniosku, że zamiarem prawodawcy unijnego było zaprojektowanie instytucji inspektora ochrony danych jako osoby proaktywnej w organizacji, tj. nie tylko informującej administratora (podmiot przetwarzający) o stanie ochrony danych osobowych w organizacji, ale również aktywnie biorącej udział w wypracowaniu rozwiązań mających umożliwić administratorowi (podmiotowi przetwarzającemu) efektywne wykonywanie obowiązków przewidzianych w przepisach o ochronie danych osobowych. IOD w założeniu ma bowiem wspierać administratora (podmiotu przetwarzającego), co potwierdza również analiza historyczna zarówno Dyrektywy 95/46/WE, którą zastąpiło RODO, jak i Ustawy z 1997 r. zastąpionej Ustawą z 2018 r.

EROD w treści Raportu wskazał cyt. „RODO nie wymyśliło koncepcji inspektora ochrony danych. Nałożyło jednak, między innymi, nowe ogólnounijne wymogi określające warunki, na jakich taki inspektor musi zostać powołany, uprawnienia, jakie taki inspektor powinien posiadać, a także szereg warunków związanych z jego pozycją w strukturze i procesach podmiotu. Przed wejściem w życie RODO Grupa Robocza Art. 29 uznała rolę inspektorów ochrony danych za "kamień węgielny odpowiedzialności", a jej Wytyczne dotyczące inspektorów ochrony danych z 2017 r. (…), które zostały zatwierdzone przez EROD po wejściu w życie RODO, stwierdziły, że będą oni "sercem tych nowych ram prawnych dla wielu organizacji"[77].

Zwrócić należy przy tym uwagę na to, że choć uchwalenie RODO, z uwagi na bezpośrednie stosowanie tego aktu, doprowadziło do istotnych zmian w obszarze ochrony danych osobowych w kraju, to ww. rozporządzenie unijne było przejawem ewolucji, a nie rewolucji w zakresie ochrony danych osobowych. RODO rozwija, a czasem powiela rozwiązania przyjęte na gruncie Dyrektywy 95/46/WE. Analizując zatem rozwiązania przewidziane w RODO, nie sposób nie korzystać z doświadczeń powstałych w okresie obowiązywania Dyrektywy 95/46/WE.

Już Dyrektywa 95/46/WE posługiwała się pojęciem „data protection official” co przetłumaczono w polskiej wersji językowej tego aktu prawnego jako „urzędnik do spraw ochrony danych osobowych”.

Nowelizacją ustawy z 1997 r. wprowadzaną ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. 2014 poz. 1662 ze zm.) prawodawca krajowy zdecydował o implementacji postanowień Dyrektywy 95/46/WE, dotyczące ww. „urzędnika”, rozbudowując i uszczegóławiając instytucję Administratora Bezpieczeństwa Informacji, wprowadzając dodatkowe zadania ABI oraz gwarantując mu niezależność w ich wykonywaniu w treści art. 36a – 36c ustawy z 1997 r.

W uzasadnieniu do tej ustawy, w zakresie w jakim odnosiła się ona do pozycji i zadań ABI wskazano m.in.: „Ze względu na powyższe wymogi prawa unijnego w zakresie dopuszczalności kompleksowego zwolnienia administratorów danych z obowiązku rejestracji zbiorów wprowadza się nowe przepisy dotyczące statusu i zadań ABI, które zapewnią zachowanie standardów wyznaczonych dyrektywą 95/46/WE, tj.: niezależność w

[77] Raport EROD, str. 8.

wykonywaniu zadań, obowiązek zapewnienia stosowania w jednostce organizacyjnej przepisów o ochronie danych osobowych, w szczególności przez przyznanie kompetencji do kontroli wewnętrznej w zakresie przestrzegania przepisów o ochronie danych osobowych, a także prowadzenie wewnętrznego rejestru zbiorów danych.”.

Niezależność, o której mowa w uzasadnieniu oraz w uchylonym art. 36a ustawy z 1997 r., prawodawca unijny sygnalizował w art. 18 ust. 2 tiret 2 - 4 Dyrektywy 95/46/WE wskazując cyt. „Dyrektywy 95/46/WE Państwa Członkowie mogą wprowadzić uproszczenie procedury lub zwolnienie z obowiązku zawiadomienia tylko w następujących sytuacjach oraz na następujących warunkach:

- jeżeli administrator danych, zgodnie z dotyczącymi go przepisami krajowymi, powoła urzędnika do spraw ochrony danych osobowych, odpowiedzialnego w szczególności:
- **za zapewnienie w niezależny sposób** wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy niniejszej dyrektywy,

  (…) ”.

ABI jako „urzędnik do spraw ochrony danych osobowych” podobnie jak IOD obecnie, miał zatem wykonywać od tej pory swoje zadania w sposób niezależny, a tę niezależność zapewniać miał mu podmiot, który go powołał. Wprowadzenie instytucji ABI w okresie obowiązywania Dyrektywy 95/46/WE stanowiło niejako przygotowanie do pełnienia funkcji IOD na gruncie RODO – trudno bowiem nie zauważyć podobieństwa w regulacji odnoszącej się ówcześnie do ABI, w porównaniu z obecnymi przepisami dotyczącymi IOD.

Na ww. kontynuację wskazują również przepisy intertemporalne ustawy z 2018 r. O następstwie polegający na ewolucji funkcji ABI do funkcji IOD świadczy, m. in. że w art. 158 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781 ze zm.) wskazano cyt. „Osoba pełniąca w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, o którym mowa w ustawie uchylanej w art. 175, staje się inspektorem ochrony danych i pełni swoją funkcję do dnia 1 września 2018 r.”. W uzasadnieniu do tej ustawy wskazano dodatkowo cyt. „Powyższe stanowiska wskazują więc skuteczny kierunek wykładni przepisów Rozporządzenia i są praktycznym drogowskazem dla inspektorów (dzisiejszych Administratorów Bezpieczeństwa Informacji”[78]. Oznacza to, że projektodawca identyfikował, iż naturalną kontynuacją funkcji ABI jest funkcja IOD.

Trzeba bowiem zwrócić uwagę, że sama funkcja IOD w polskim porządku prawnym, zastąpiła funkcję Administratora Bezpieczeństwa Informacji.

Potwierdzają to również stanowiska doktryny: „Wobec braku przepisów przejściowych w rozporządzeniu 2016/679 polski ustawodawca, dostrzegając potrzebę uregulowania międzyczasowego m.in. w zakresie regulacji administratorów bezpieczeństwa informacji, która w istotnych elementach była zbliżona konstrukcyjnie do przepisów dotyczących inspektorów danych osobowych w rozporządzeniu ogólnym, zdecydował się na przyjęcie następstwa prawnego dla osób pełniących dotychczas funkcję administratorów bezpieczeństwa informacji

[78] Uzasadnienie do ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781 ze zm.) str. 13

i uznanie ich za inspektorów ochrony danych w rozumieniu przepisów rozporządzenia 2016/679 wraz z rozpoczęciem stosowania rozporządzenia[79]".

RODO ustala status i rolę IOD jako osoby profesjonalnej, posiadającą niezbędną fachową wiedzę do wykonywania zadań opisanych w RODO, która stale podnosi swoje kompetencje w obszarze ochrony danych osobowych. Nadrzędnym celem funkcji IOD jest jednak wsparcie administratora (podmiotu przetwarzającego), w przestrzeganiu przepisów prawa z obszaru ochrony danych osobowych. Podobną rolę przewidywała dla ówczesnego „urzędnika do spraw ochrony danych osobowych" Dyrektywa 95/46/WE, który odpowiedzialny był za zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy tej dyrektywy.

Zauważyć jednak trzeba, że zarówno na gruncie Dyrektywy 95/46/WE, jak i na podstawie RODO prawodawca nie dookreślił w jaki sposób IOD (urzędnik do spraw ochrony danych osobowych) w praktyce ma doradzać administratorowi (podmiotowi przetwarzającemu) oraz wspierać go w realizacji obowiązków przewidzianych w przepisach o ochronie danych osobowych.

Z uwagi na powyższe w ocenie autora opinii możliwe jest wyodrębnienie dwóch podstawowych modeli pełnienia funkcji IOD:

a. model statyczny

b. model dynamiczny

- przy czym każdy z tych modeli jest dopuszczalny i prawidłowy, choć realizowanie każdego z nich wiąże się z innymi ryzykami dla organizacji. W modelu dynamicznym możliwy jest również różny stopień aktywności IOD, co wyjaśniam w dalszej części.

Model statyczny

Wykonywanie funkcji IOD w modelu statycznym polega w głównej mierze na monitorowaniu wykonywania i przestrzegania przez administratora (podmiot przetwarzający) przepisów o ochronie danych osobowych, informowaniu o dostrzeżonych uchybieniach oraz podejmowaniu działań (w tym szkoleń) podnoszących ogólną świadomość w obszarze ochrony danych osobowych w organizacji. Zadanie IOD doradzania i informowania właśnie koncentruje się na tymże podnoszeniu świadomości w organizacji. Kluczowe dla tego modelu jest założenie, że IOD nie może monitorować szczegółowych rozwiązań, które sam zaproponował.

Model statyczny zakłada, że IOD nie podejmuje działań, które mogłyby mieć jakikolwiek wpływ na rozwiązania przyjmowane przez administratora (podmiot przetwarzający) w organizacji. IOD wskaże, że określone rozwiązanie nie jest prawidłowe oraz przyczyny takiego stanowiska, jednak bez dookreślania konkretnego rozwiązania, potencjalnie niezawierającego wady jaką obarczone jest rozwiązanie pierwotne (np. opracowania treści dokumentu, którego wadliwość się wskazało w trakcie monitorowania/audytu).

Ewentualne dodatkowe zadania IOD ograniczają się do czynności dokumentacyjnych i technicznych, takich jak:

[79] D. Lubasz, w: E. Bielak-Jomaa, I. Bogucka, W. Chomiczewski, P. Drobek, M. Gawroński, U. Góral, K. Kloc, J. Łuczak-Tarka, P. Punda, N. Zawadzka, M. Żmijewski, D. Lubasz, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2019, art. 158.

- prowadzenie RCP,

- prowadzenie RCKP,

- dokumentowanie naruszeń,

- techniczne przesyłanie pism administratora do osób, których dane dotyczą oraz do organu nadzorczego.

Niewątpliwie istnieją organizacje, w których ograniczenie statusu IOD wyłącznie do monitorowania ochrony danych osobowych w organizacji i informowanie o niej kierownictwo, wraz z działaniami podnoszącymi ogólną świadomość ochrony danych osobowych w organizacji będzie wystarczające i umożliwi wsparcie obowiązków administratora (podmiotu przetwarzającego) określonych w RODO.

Istnieje jednak ryzyko, że w przypadku konieczności reakcji na daną okoliczność lub zdarzenie administrator (podmiot przetwarzający) nie będzie w stanie prawidłowo zareagować na np. naruszenie ochrony danych osobowych, podejmując środki naprawcze.

Tego rodzaju model może wymagać zatrudnienia przez administratora (podmiot przetwarzający) dodatkowej osoby/zespołu osób, wyspecjalizowanej/wyspecjalizowanych w ochronie danych osobowych i niebędącej IOD w celu realizacji obowiązków przewidzianych w RODO, które realizować ma administrator (podmiot przetwarzający). Dzięki temu podmiot otrzyma propozycję rozwiązań nieprawidłowości stwierdzonych przez IOD oraz będzie podejmował decyzję o ich zastosowaniu, po otrzymaniu stanowiska IOD w tym przedmiocie.

Model statyczny zmniejsza jednocześnie ryzyko wystąpienia konfliktu interesów o charakterze merytorycznym.

Model dynamiczny

W modelu dynamicznym IOD nie ogranicza się do wsparcia administratora tylko do prowadzenia działań polegających na monitorowaniu i informowaniu poprzez proponowanie mu określonych rozwiązań w organizacji, lecz również podejmuje szersze działania wspierające administratora (podmiot przetwarzający). Zastrzec jednak trzeba, że w tym modelu IOD nie podejmuje ostatecznej decyzji, np. co do treści określonej procedury postępowania z danymi osobowymi, treści odpowiedzi do podmiotu danych czy treści zgłoszenia naruszenia, w przypadku obowiązku zgłoszenia go do Prezesa UODO.

W modelu dynamicznym zadania IOD obejmują zarówno kwestie związane z monitorowaniem ochrony danych osobowych w organizacji i podnoszeniem ogólnej świadomości w organizacji, z obszaru ochrony danych osobowych, jak i informowanie oraz doradzanie administratorowi (podmiotowi przetwarzającemu) w kwestiach związanych z ochroną danych osobowych w organizacji. Aspekt doradzania administratorowi jest rozumiany szeroko, w związku z czym IOD w modelu dynamicznym, np. stwierdzając uchybienie w organizacji przedstawia możliwe konkretne sposoby rozwiązania problemów, czy też w zakresie przyszłych działań proponuje konkretne rozwiązanie. W modelu dynamicznym akcent zostaje położony na tym, że funkcje „doradzania" i „monitorowania" są równorzędnymi zadaniami IOD i nie można ograniczać żadnej z nich kosztem drugiej, szczególnie biorąc pod uwagę kwalifikacje IOD i jego misję jak najdalej idącego wspierania administratora (podmiotu przetwarzającego).

Podkreślenia w tym miejscu wymaga, że zgłaszanie przez IOD możliwych wariantów rozwiązań nie może oznaczać faktycznego zastępowania administratora (podmiotu

przetwarzającego) w podejmowaniu decyzji o ostatecznym kształcie rozwiązania lub jego wdrożeniu. Zauważyć też trzeba, że z doradzaniem administratorowi związane jest zajęcie przez IOD stanowiska, co do stosowanych w organizacji rozwiązań lub planowanych działań, co powinno mieć wpływ na ostateczną decyzję administratora co do prowadzonego lub planowanego procesu przetwarzania danych osobowych.

Istotne jest jednak, że to nie IOD podejmuje tę decyzję i nie on odpowiada za kształt ostatecznego rozwiązania. W tym modelu IOD działa proaktywnie, czynnie wspierając administratora (podmiot przetwarzający) w stosowaniu przepisów o ochronie danych osobowych w organizacji. Konieczne jest jednak zapewnienie rozliczalności funkcji IOD, polegające na wykazaniu, że rola najwyższego kierownictwa administratora (podmiotu przetwarzającego) nie sprowadza się wyłącznie do zatwierdzenia rozwiązań wskazanych przez IOD. W przeciwnym wypadku uzasadniona będzie teza o fikcji decydowania przez administratora o celach i sposobach przetwarzania danych osobowych w ww. zakresie. Będzie to bowiem faktyczna decyzja IOD pociągająca za sobą występowanie konfliktu interesów o charakterze merytorycznym.

W modelu dynamicznym IOD posiada większą inicjatywę niż w przypadku modelu statycznego. W przypadku realizowania zadań przez IOD w modelu dynamicznym istnieje wyższe ryzyko stwierdzenia konfliktu interesów z uwagi na większe zaangażowanie IOD w sprawy dotyczące ochrony danych osobowych w organizacji, niż ma to miejsce w modelu statycznym.

Taki model wymaga więc udokumentowania i rzeczywistego wykazania, że zaangażowanie IOD nie stanowi faktycznego decydowania o celach i sposobach przetwarzania danych osobowych.

Ewentualne dodatkowe zadania IOD mogą w tym modelu polegać m. in. na:

- czynnościach dokumentacyjnych (prowadzenie RCP, prowadzenie RCKP, dokumentowanie naruszeń) oraz czynnościach technicznych (np. przesyłanie pism administratora do osób, których dane dotyczą, czy do organu nadzorczego),
- przedstawieniu propozycji polityki ochrony danych osobowych oraz innych dokumentów wewnętrznych administratora i dalszych wykonujących jego obowiązki (np. klauzul informacyjnych wobec osób, których dane dotyczą),
- przedstawieniu propozycji rozwiązań zapobiegających wystąpieniu naruszenia w przyszłości,
- przedstawienie szablonów odpowiedzi na wnioski podmiotów danych, dostosowywanych następnie przez administratora do faktycznie otrzymywanych wniosków.

W tym modelu szeroko możemy także rozumieć wykonywanie własnych zadań przez IOD (doradzania administratorowi), w których z własnej inicjatywy może on brać udział:

- w rozpatrywaniu wniosków osób, których dane dotyczą, przez przedstawianie własnej oceny, stanowiska, a nawet propozycji określonego sposobu załatwienia sprawy,
- w zarządzaniu naruszeniem ochrony danych, w tym przez przedstawianie własnej oceny, stanowiska co do naruszenia i propozycji konkretnych działań,

– w innych konkretnych sprawach z zakresu ochrony danych osobowych, w których przedstawia własne stanowisko (np. co do zawieranych umów powierzenia przetwarzanych danych).

W żadnym z tych działań IOD nie podejmuje jednak decyzji o ostatecznym kształcie wykonywania obowiązku przez administratora.

Należy jednak pamiętać, że w modelu dynamicznym może wystąpić różny stopień aktywności IOD (zakres aktywnych zadań IOD), także w praktyce mogą wystąpić różne jego warianty (np. przejście z modelu statycznego tylko w zakresie rekomendacji działań po zarządzeniu naruszeniem ochrony danych). Zakres tej aktywności ustala: administrator (podmiot przetwarzający) w przypadku zadań dodatkowych, ale także sam IOD w przypadku „zadań własnych" przewidzianych dla niego w RODO.

3. Wnioski

3.1 Celem unikania konfliktu interesów jest zapewnienie prawidłowości wykonywanego zawodu lub funkcji. Konsekwencją konfliktu interesów jest brak niezależności i obiektywizmu w pełnieniu funkcji oraz wykonywanie jednocześnie zadań na zlecenie podmiotów, które mają lub mogą mieć sprzeczne ze sobą interesy w danym obszarze.

3.2 Pojęcie „konflikt interesów" oznacza istnienie kolidującego z głównym interesem polegającym ma prawidłowym realizowaniu zadania (np. wykonywanie zawodu czy funkcji) innego interesu (lub interesów) tej samej osoby, czyli taki (takie), które uniemożliwiają prawidłowe działanie.

3.3 Pod pojęciem „prawidłowe działania" (prawidłowego wykonywani zadania) rozumiem działanie według przyjętego w prawie lub zasadach etycznych wzorca postępowania. Takim wzorem może być postępowanie niezależne, bezstronne, obiektywne, bezinteresowne lub lojalne wobec klienta. Interesy kolidujące z tym wzorcem są związane z sytuacją osobistą wykonującego zadania (jego własną lub dotyczącą osób najbliższych) lub innymi wartościami (interesami), które realizuje ta osoba (np. nakierowanie na inne cele niż wymienione powyżej, choćby lojalność wobec innych podmiotów).

3.4 Konflikt interesów w wykonywaniu funkcji IOD o którym mowa w art. 38 ust. 6 RODO ma charakter częściowo autonomiczny. Konflikt ten występuje w sytuacji, jeżeli inne nałożone na IOD zadania i obowiązki uniemożliwiają prawidłowe wykonywanie zadań IOD określonych w art. 39 RODO.

3.5 Przez prawidłowe wykonywanie zadań IOD rozumiem ich realizowanie w sposób niezależny, obiektywny oraz skuteczny.

3.6 Występowanie konfliktu interesów wykonywania funkcji IOD ma charakter obiektywny i jest uzależniony od okoliczności faktycznych, które musza zostać wzięte pod uwagę przy ocenie, czy sposób oraz warunki zarówno wykonywania zadań IOD będzie prowadzić do rzeczywistego konfliktu interesów.

3.7 Zasadą jest, że IOD może wykonywać dodatkowe zadania i obowiązki. Wyjątkową sytuacją jest natomiast występowanie konfliktu interesów, który będzie uniemożliwiał wykonywanie jednocześnie dodatkowych zadań i prawidłowe sprawowanie funkcji IOD.

Kwalifikację sytuacji powodującej konflikt interesów na gruncie przepisów o ochronie danych osobowych należy wykładać wąsko.

3.8 W ocenie autora niniejszej opinii możliwe jest wykonywanie funkcji IOD w dwóch modelach, tj. statycznej i dynamicznej:

1) **Model statyczny** zakłada, że rolą IOD w organizacji jest przede wszystkim monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz zasad przyjętych w organizacji i sygnalizowanie nieprawidłowości, jednak bez wskazywania konkretnych możliwych rozwiązań dostrzeżonych uchybień. Rolą IOD jest również podnoszenie świadomości w obszarze ochrony danych osobowych w organizacji („budowanie świadomości"). Doradzanie, będące jednym z zadań IOD sprowadza się do podnoszenia świadomości samego administratora (podmiotu przetwarzającego) jak i jego personelu, w obszarze ochrony danych osobowych. Rozwiązanie to może wymagać zaangażowania dodatkowego podmiotu w celu skonkretyzowanej realizacji obowiązków przewidzianych w RODO (tj. wparcia w tym zakresie administratora), jednak wiąże się z niższym ryzykiem występowania konfliktu interesów funkcji IOD.

   Ewentualne dodatkowe zadania IOD ograniczają się do czynności dokumentacyjnych, takich jak:

   - prowadzenie RCP,

   - prowadzenie RCKP,

   - dokumentowanie naruszeń,

   jak również do czynności technicznych, np. takich jak przesyłanie pism administratora do osób, których dane dotyczą, czy do organu nadzorczego.

2) **Model dynamiczny** zakłada, że IOD nie tylko monitoruje przestrzeganie przepisów o ochronie danych osobowych oraz zasad przyjętych w organizacji i sygnalizuje nieprawidłowości, ale też bierze aktywny udział w rozwiązaniu stwierdzonych uchybień i problemów w zakresie przyszłych działań, poprzez przedstawienie konkretnych możliwych rozwiązań administratorowi, chociaż co ważne, nie decyduje o ich ostatecznym kształcie i nie wdraża ich. Rozwiązanie to zakłada większą aktywność IOD w organizacji, jednak wiąże się większym ryzykiem wystąpienia konfliktu interesów, co wymaga ustanowienia gwarancji niezależności, obiektywizmu i skuteczności w zasadach wewnętrznych w organizacji. Model ten jest wielowariantowy, ponieważ różny może być przewidziany w nim zakres aktywności IOD.

   Ewentualne dodatkowe zadania IOD mogą polegać m. in. na:

   - czynnościach dokumentacyjnych (prowadzenie RCP, prowadzenie RCKP, dokumentowanie naruszeń),
   - przedstawieniu propozycji polityki ochrony danych osobowych oraz innych dokumentów wewnętrznych administratora i dalszych wykonujących jego obowiązki (np. klauzul informacyjnych wobec osób, których dane dotyczą),
   - przedstawieniu propozycji rozwiązań zapobiegających wystąpieniu naruszenia w przyszłości,

- przedstawienie szablonów odpowiedzi na wnioski podmiotów danych, dostosowywanych następnie przez administratora do faktycznie otrzymywanych wniosków.

11. W ocenie autora oba modele są możliwe do zastosowania przez administratora lub podmiot przetwarzający w swojej organizacji. W obszarze ochrony danych osobowych administrator (podmiot przetwarzający) przy nakładaniu dodatkowych zadań może wziąć pod uwagę to, że głównym celem istnienia i aktywności IOD jest jego wsparcie - w dopuszczalnym zakresie - w realizacji obowiązków ustalonych w RODO, w szczególności zważywszy na kwalifikacje zawodowe IOD, które są podstawą jego wyznaczenia. Granicą tych dodatkowych zadań jest naruszenie nimi niezależności, obiektywizmu i skuteczności działań IOD.

Signature Not Verified
Dokument podpisany przez Grzegorz Sibiga
Data: 2024.04.08 10:32:05 CEST

dr hab. Grzegorz Sibiga

prof. INP PAN

Załączniki:

1) Wykaz źródeł
2) Stanowiska organu ochrony danych osobowych dotyczące konfliktu interesów IOD

Załącznik nr 1 - Wykaz źródeł

Akty prawne

- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. L. z 1995 Nr 281, str. 31–50)
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L. z 2016 r. nr 119, str. 1, z późn. zm.);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. U. UE. L. z 2018 r. Nr 295, str. 39).
- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. 2023 poz. 775 ze zm.);
- Ustawa z dnia 5 lipca 1996 r. o doradztwie podatkowym (Dz. U. z 2021 r. poz. 2117)
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 poz. 922)
- Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781 ze zm.)
- Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (Dz. U. z 2022 r. poz. 1166 z późn. zm.)
- Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. 2023 poz. 1634 ze zm.)
- Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. 2023 poz. 1605 ze zm.)
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015 poz. 719, uchylone)

Teksty urzędowe

- CNIL. “Guide on data protection officers”, dostępny pod adresem URL: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf (dostęp: 2.04.2024 r.)
- Decyzja ADP (Belgia) Proximus z dnia 28 kwietnia 2020 r.
- Decyzja APD (Belgia) z dnia 16 grudnia 2021 r., nr 141/2021
- Decyzja CNPD (Luksemburg) z dnia 13 października 2021 r., 36FR/2021
- Decyzja APD (Belgia) z dnia 13 października 2021 r., nr 37FR 2021

- Decyzja APD (Belgia) z dnia 28 maja 2020 r., nr 18/2020
- DPC. Guidance Note: Records of Processing Activities (RoPA) under Article 30 GDPR, dostępny pod adresem URL: https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Records%20of%20Processing%20Activities%20%28RoPA%29%20under%20Article%2030%20GDPR.pdf, (dostęp: 5.04.2024 r.)
- EDPB. Guide for small business, dostępny pod adresem URL: https://edpb.europa.eu/sme-data-protection-guide/data-protection-officer_en (dostęp: 5.04.2024 r.)
- Kodeks Etyki Radcy Prawnego stanowiący załącznik do uchwały nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014 r. uwzględniający zmiany wprowadzone uchwałą Nr 1/2022 Krajowego Zjazdu Radców Prawnych z dnia 8 lipca 2022 r. w sprawie zmiany Kodeksu Etyki Radcy Prawnego
- Komunikat Prezesa UODO z 3.11.2021 r. dostępny pod adresem URL: https://uodo.gov.pl/pl/495/2415 (dostęp: 5.04.2024 r.)
- Komunikat Prezesa UODO z 15.01.2019 Prezesa UODO dostępny pod adresem URL: https://archiwum.uodo.gov.pl/pl/225/659 (dostęp: 5.04.2024 r.)
- Komunikat Prezesa UODO z 30.03.2022 r. Prezesa UODO dostępny pod adresem URL: https://uodo.gov.pl/pl/138/2438 (dostęp: 5.04.2024 r.)
- Komunikat Prezesa UODO z 10.05.2022 r. Prezesa UODO dostępny pod adresem URL:https://archiwum.uodo.gov.pl/pl/225/2374 (dostęp: 5.04.2024 r.)
- Komunikat Prezesa UODO z 17.01.2024 r. Prezesa UODO dostępny pod adresem URL: https://uodo.gov.pl/pl/138/2438 (dostęp: 5.04.2024 r.)
- Komunikat CNIL “Record of processing activities” z dnia 19.08.2019 r., dostępny pod adresem URL: https://www.cnil.fr/en/record-processing-activities (dostęp: 5.04.2024 r.)
- Komunikat łotewskiego organu nadzorczego z zakresu ochrony danych osobowych z dnia 19.08.2022 r. “Datu aizsardzības speciālista funkcijas un uzdevumi”, dostępny pod adresem URL: https://www.dvi.gov.lv/lv/jaunums/dviskaidro-DAS_190822, (dostęp: 5.04.2024 r.)
- Komunikat na stronie internetowej Guide to completing the record of processing activities, dostępny pod adresem URL: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2d_en/page2d_en?opendocument, (dostęp: 5.04.2024 r.)
- Komunikat EIOD “Data Protection Officer (DPO)”, dostępny pod adresem URL: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (dostęp: 5.04.2024 r.)
- Komunikat Komisji Europejskiej dostępny pod adresem URL: https://commission.europa.eu/about-european-commission/service-standards-and-principles/transparency/data-processing-register_en (dostęp: 5.04.2024 r.)
- Komunikat Prezesa UODO z 15 stycznia 2019 dostępny obecnie pod adresem URL:https://archiwum.uodo.gov.pl/pl/225/659 (dostęp: 5.04.2024 r.)

- Raport Europejskiej Rady Ochrony Danych przyjęty 16 stycznia 2024 r. w ramach skoordynowanego działania egzekwowania prawa (CEF) w 2023 r., dotyczącego wyznaczenia i pozycji inspektorów ochrony danych, dostępny pod adresem URL:
- Rozmowa z ekspertem. “Dorobek orzeczniczy powinien kształtować standardy, mając na uwadze troskę o obywatela – Jacek Młotkiewicz, dyrektor Departamentu Kontroli i Naruszeń w UODO “[w:] Biuletyn UODO nr 2/04/23, https://uodo.gov.pl/pl/file/4302 (dostęp: 2.04.2024 r.)
- Sprawozdanie krajowe Prezesa UODO w ramach badania prowadzonego przez EROD w ramach skoordynowanego działania egzekwowania prawa (CEF) w 2023 r., dotyczącego wyznaczenia i pozycji inspektorów ochrony danych dostępne pod adresem URL: https://uodo.gov.pl/pl/138/2960 (dostęp: 5.04.2024 r.)
- UODO sygnalizuje. “Za realizację praw osób w zakresie dostępu do dotyczących ich danych odpowiada administrator” [w:] Biuletyn UODO Nr 01/01/24, https://uodo.gov.pl/pl/file/4602 (dostęp: 5.04.2024 r.)
- Uzasadnienie do ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. 2014 poz. 1662 ze zm.)
- Uzasadnienie do ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781 ze zm.)
- Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (WP 243 rew. 01)
- Wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250)
- Wytyczne EROD z 28 marca 2023 nr 09/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych zgodnie z RODO
- Załącznik do uchwały nr 12/2022 Krajowej Rady Doradców Podatkowych z dnia 14 lutego 2022 r. w sprawie przyjęcia tekstu jednolitego Zasad etyki doradców podatkowych - Zasady Etyki Doradców Podatkowych
- Zbiór Zasad Etyki Adwokackiej i Godności Zawodu (Kodeks Etyki Adwokackiej)

Literatura

- *D. Korff, M. Georges,* Podręcznik Inspektora Ochrony Danych. Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi publicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych, 2019
- *A. Dyczkowski*, red., Nowy Leksykon PWN, Warszawa 1998
- *Encyklopedia powszechna PWN*, t. II, Warszawa 1984
- *E. Bielak-Jomaa (red.), D. Lubasz (red.),* RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018

- *E. Bielak-Jomaa, I. Bogucka, W. Chomiczewski, P. Drobek, M. Gawroński, U. Góral, K. Kloc, J. Łuczak-Tarka, P. Punda, N. Zawadzka, M. Żmijewski, D. Lubasz*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2019
- *E. Bielak – Jomaa, P. Drobek, D. Krajewska-Kekusz M. Młotkiewicz M. Kawecki, T. Soczyński, A. Kaczmarek K. Hildebrandt*, Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych, Warszawa 2016
- *E. Maniewska, K. Jaśkowski*, Kodeks pracy. Komentarz aktualizowany, LEX/el. 2024
- *H. Hamer*, Psychologia społeczna. Teoria i praktyka, Warszawa 2005
- *K. Kwapisz*, Ustawa o radcach prawnych. Komentarz, Warszawa 2011
- *J. L. Bernat, H. R. Beresford*, red., Handbook of Clinical Neurology, 2013
- *R. Chadwick* ,red., Encyclopedia of Applied Ethics (Second Edition), Academic Press, 2012
- *J. Naumann,* Zbiór Zasad Etyki Adwokackiej i Godności Zawodu. Komentarz. Wyd. 5, Warszawa 2023
- *J. Pieńkos*, Słownik łacińsko-polski. Łacina w nauce i kulturze, Warszawa 1996
- *J. Sondel*, Słownik łacińsko-polski, Kraków 2009
- *J. Wojnowski*, red., Wielka Encyklopedia PWN, red. J. Wojnowski, t. XII, Warszawa 2002
- *M. Hoskins,* how to be a decent DPO: letters to aspiring privacy pros, 2021
- M. Chrzanowski, J. Kostrubiec, I. Nowikowski, red., Państwo, prawo, polityka. Księga poświęcona pamięci Profesora Henryka Groszyka, Lublin 2012
- *M. Szymczak*, red., Słownik języka polskiego PWN, Wydawnictwo Naukowe PWN Warszawa 1996, tom I A-K
- *P. De Hert, I. Spiecker gen. Döhmann, V. Papakonstantinou* (red.), General Data Protection Regulation Article-by-Article Commentary, Baden-Baden 2023
- *P. Grosmann,* Die Interessenkonflikte der betrieblichen und behördlichen Datenschutzbeauftragten, Heidelberg 2024
- *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II, Warszawa 2022
- *S. Dubiosz*, red., Uniwersalny słownik języka polskiego, Wydawnictwo Naukowe PWN, Warszawa 2008, tom K-Ó.
- *Słownik języka polskiego PWN*, w opracowaniu E. Sobol i innych, Wydawnictwo Naukowe PWN, Warszawa 2011
- *T. Scheffler,* red., Kodeks Etyki Radcy Prawnego. Komentarz. Wyd. 4, Warszawa 2023

Załącznik nr 2 - Stanowiska organu ochrony danych osobowych dotyczące konfliktu interesów IOD

A. Stanowiska wyrażane na stronie internetowej organu

1. Stanowisko z 20 grudnia 2017

„Podobnie jak ma to miejsce na gruncie aktualnie obowiązującej ustawy o ochronie danych osobowych (art. 36a ust. 8 **Ustawa z 1997 r.**) inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora, czy też nie – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób **niezależny** (motyw 97 RODO). W celu zapewnienia niezależności DPO administrator lub podmiot przetwarzający powinni wprowadzić wewnętrzne regulacje gwarantujące inspektorowi ochrony danych niezależność w wykonywaniu przez niego obowiązków i zadań. Odnosi się to w szczególności do podmiotów publicznych czy też podmiotów o złożonych strukturach, które będą musiały dostosować swoje regulaminy organizacyjne oraz statuty tak, aby zapewnić niezależność DPO. Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektora ochrony danych umiejscowienie inspektora ochrony danych w strukturze organizacyjnej danego podmiotu powinno być czytelne dla całego personelu administratora lub podmiotu przetwarzającego, w związku z czym w przypadku powołania DPO, administrator lub podmiot przetwarzający powinien zawiadomić o tym fakcie pozostałych pracowników. W celu zapewnienia niezależności inspektorowi ochrony danych ogólne rozporządzenie o ochronie danych, wprowadza kilka szczegółowych rozwiązań, które pozwalają na osiągnięcie ww. celu, mianowicie:

(…)

5. Zgodnie z art. 38 ust. 6 RODO, istnieje możliwość nakładania na inspektora ochrony danych innych zadań i obowiązków, ale administrator i podmiot przetwarzający muszą zapewnić by nie powodowało to konfliktu interesów. Zatem jak wyjaśnia Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych oznacza to m.in., że DPO nie może zajmować w organizacji stanowiska związanego z określaniem sposobów i celów przetwarzania danych. Aspekt ten powinien być analizowany osobno i indywidualne dla każdego podmiotu. Powierzając inspektorowi ochrony danych inne zadania, w celu uniknięcia konfliktu interesów administrator danych lub podmiot przetwarzających, powinni w swojej organizacji zidentyfikować stanowiska niekompatybilne z pełnieniem funkcji DPO.
Cenną podpowiedzią w tym zakresie jest wskazanie, że co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych. Ponadto konflikt interesów może powstać wówczas, gdy zewnętrzny DPO zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych. Wskazane byłoby też opracowanie wewnętrznej polityki określającej stanowiska będące w konflikcie interesów oraz opracowanie generalnego dokumentu dotyczącego konfliktu interesów. Ponadto administrator lub podmiot przetwarzający powinni wprowadzić odpowiednie zabezpieczenia do wewnętrznych zasad organizacji celem zapewnienia, by ogłoszenia o rekrutacji na stanowisko inspektora ochrony danych były sformułowane w jasny, precyzyjny sposób i niwelowały ryzyko powstania konfliktu interesów.”
https://web.archive.org/web/*/https://abi.giodo.gov.pl/inspektor-ochrony-danych/gwarancje-niezaleznosci (dostęp: 2.04.2024)

2. Stanowisko z 22 maja 2018 r.

„Wprawdzie z art. 30 rozporządzenia ogólnego bezsprzecznie wynika, że obowiązek prowadzenia rejestrów należy do administratorów i podmiotów przetwarzających, nie zaś do inspektora ochrony danych, niemniej trudno sobie wyobrazić, że inspektor ochrony danych - jako osoba dysponująca odpowiednią wiedzą i umiejętnościami w dziedzinie ochrony danych osobowych - nie będzie angażowała się w tworzenie i prowadzenie rejestrów, a następnie wykorzystywała ich w swojej pracy. Inspektor ochrony danych jako fachowiec może wspomagać administratora w tworzeniu i prowadzeniu rejestrów na przykład poprzez zbieranie informacji w celu identyfikacji procesów przetwarzania." https://archiwum.uodo.gov.pl/pl/122/199 (dostęp: 2.04.2024)

3. Stanowisko z 15 stycznia 2019 r.

„Ze względu na swoją zawartość i cele, rejestry czynności oraz rejestry kategorii czynności mogą być również przydatnym instrumentem monitorowania zgodności dla inspektorów ochrony danych. Wprawdzie z art. 30 rozporządzenia ogólnego bezsprzecznie wynika, że obowiązek prowadzenia rejestrów należy do administratorów i podmiotów przetwarzających, nie zaś do inspektora ochrony danych, niemniej trudno sobie wyobrazić, że inspektor ochrony danych - jako osoba dysponująca odpowiednią wiedzą i umiejętnościami w dziedzinie ochrony danych osobowych - nie będzie angażowała się w tworzenie i prowadzenie rejestrów, a następnie wykorzystywała ich w swojej pracy.

Inspektor ochrony danych jako fachowiec może wspomagać administratora w tworzeniu i prowadzeniu rejestrów na przykład poprzez doradzanie mu w kwestiach związanych z wykonaniem tego obowiązku." https://archiwum.uodo.gov.pl/pl/225/659 (dostęp: 2.04.2024)

4. Stanowisko z 7 stycznia 2019 r.

„Zgodnie z art. 24 RODO administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Treść powyższego artykułu wskazuje jednoznacznie, że wdrożenie odpowiednich środków technicznych i organizacyjnych (które mogą obejmować również wdrożenie przez administratora odpowiednich polityk ochrony danych) należy do obowiązków administratora (osób przez niego wyznaczonych). Rolą IOD jest natomiast dokonywanie oceny przyjętych przez administratora środków (w tym wewnętrznych polityk) pod kątem ich zgodności z przepisami prawa i skuteczności. Do zadań inspektora ochrony danych należy też monitorowanie przestrzegania przyjętej w dziedzinie ochrony danych osobowych polityki przez osoby upoważnione do przetwarzania danych (art. 39 ust 1 lit. b RODO). W trakcie tworzenia polityk dotyczących ochrony danych wskazane jest, aby administrator zasięgał opinii i wskazówek u swojego inspektora ochrony danych (IOD), który posiada fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych, zgodnie z treścią art. 39 ust 1 lit. a RODO" https://archiwum.uodo.gov.pl/pl/225/634 (dostęp: 2.04.2024)

5. Stanowisko z 11 lutego 2019 r.

„Zgodnie z art. 38 ust. 6 RODO, istnieje możliwość nakładania na inspektora ochrony danych innych zadań i obowiązków, ale administrator i podmiot przetwarzający muszą zapewnić by nie powodowało to konfliktu interesów. Zatem jak wyjaśnia Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych oznacza to m.in., że IOD nie może zajmować w organizacji stanowiska związanego z określaniem sposobów i celów przetwarzania danych. Aspekt ten powinien być analizowany osobno i indywidualne dla

każdego podmiotu. Powierzając inspektorowi ochrony danych inne zadania, w celu uniknięcia konfliktu interesów administrator danych lub podmiot przetwarzających, powinni w swojej organizacji zidentyfikować stanowiska niekompatybilne z pełnieniem funkcji IOD. Cenną podpowiedzią w tym zakresie jest wskazanie, że co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych. Ponadto konflikt interesów może powstać wówczas, gdy zewnętrzny IOD zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych. Wskazane byłoby też opracowanie wewnętrznej polityki określającej stanowiska będące w konflikcie interesów oraz opracowanie generalnego dokumentu dotyczącego konfliktu interesów. Ponadto administrator lub podmiot przetwarzający powinni wprowadzić odpowiednie zabezpieczenia do wewnętrznych zasad organizacji celem zapewnienia, by ogłoszenia o rekrutacji na stanowisko inspektora ochrony danych były sformułowane w jasny, precyzyjny sposób i niwelowały ryzyko powstania konfliktu interesów." https://archiwum.uodo.gov.pl/pl/223/713 (dostęp: 2.04.2024)

6. Stanowisko z 3 listopada 2021 r.

„Konflikt interesów następuje, jeśli nie można pogodzić prawidłowego wykonywania zadań IOD z realizacją innych zadań, gdyż pomiędzy zadaniami występuje sprzeczność, uniemożliwiająca odpowiednią ich realizację. Konflikt interesów może być również rezultatem nadmiaru obowiązków przydzielonych do wykonania IOD, jeśli IOD musi wybrać między obowiązkami, jakie będzie realizował, a tymi, którym nie podoła z powodu braku czasu koniecznego na ich wykonanie. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Oznacza to, że IOD nie może zajmować w organizacji stanowiska, na którym określa się sposoby i cele przetwarzania danych. W powołanych wyżej Wytycznych dotyczących IOD wskazane zostały przykłady takich stanowisk. Należą do nich: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli sprawujące je osoby biorą udział w określaniu celów i sposobów przetwarzania danych. Ocena, czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana indywidualnie z uwzględnieniem konkretnych okoliczności. Oznacza to, że możliwość zaistnienia konfliktu powinna być stale monitorowana, ponieważ przyczyny zaistnienia takiego konfliktu mogą występować również w późniejszym czasie, po rozpoczęciu pełnienia funkcji przez IOD." https://uodo.gov.pl/pl/495/2415 (dostęp: 2.04.2024)

7. Stanowisko z 10 maja 2022 r.

„Kształtując zatem zakres obowiązków IOD warto pamiętać, że inspektor nie powinien realizować zadań, które mogą stać się następnie przedmiotem dokonywania przez niego czynności monitorowania ani podejmować decyzji w zakresie celów i środków dotyczących przetwarzania i zabezpieczania danych. Z konfliktem interesów mielibyśmy do czynienia również wówczas, gdyby IOD miał w imieniu administratora sporządzać projekty umów powierzenia przetwarzania danych osobowych. Najpierw bowiem określałby, w jaki sposób ukształtowane będą relacje między administratorem i podmiotem przetwarzającym oraz prawa i zobowiązania stron umowy, a następnie, realizując swoje obowiązki, zobowiązany byłby jednocześnie ocenić prawidłowość i zgodność z przepisami podjętych w tym zakresie decyzji." https://archiwum.uodo.gov.pl/pl/225/2374 (dostęp: 2.04.2024)

B. Stanowiska zawarte w decyzjach opublikowanych na stronie internetowej organu

8. Decyzja Prezesa UODO sygn. ZWAD.405.31.331.2019

„Podstawowy zakres zadań IOD, wśród których na próżno szukać jednak tych związanych z nadawaniem pracownikom administratora upoważnień do przetwarzania danych osobowych, określony został przez unijnego ustawodawcę w art. 39 ust. 1 rozporządzenia 2016/679, niemniej jednak zgodnie z art. 38 ust. 6 ww. rozporządzenia IOD może wykonywać też inne zadania i obowiązki, o ile administrator lub podmiot przetwarzający zapewni, aby te zadania i obowiązki nie powodowały konfliktu interesów. Należy jednak przyjąć, że z uwagi na specyfikę zadań IOD ogniskujących się na doradzaniu oraz kontrolowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych, administrator nie powinien przyznawać IOD uprawnień do nadawania w jego imieniu upoważnień do przetwarzania danych osobowych, pozostawiając IOD w procedurze wydawania upoważnień do przetwarzania danych osobowych sprawowanie funkcji doradczej i nadzorczej. Przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny za przeprowadzenie tej procedury, a jednocześnie miałby monitorować jej zgodność z przepisami o ochronie danych osobowych, do czego zobowiązuje go unormowanie zawarte w art. 39 ust. 1 lit. b) rozporządzenia 2016/679, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów, czego wprost zakazuje art. 38 ust. 6 rozporządzenia 2016/679. Wyraźnego podkreślenia wymaga fakt, iż IOD, cechujący się szczególnym statusem w dziedzinie zapewniania właściwego przestrzegania przepisów o ochronie danych osobowych, musi mieć dla tego celu zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na efektywną, niezależną oraz prawidłową realizację obowiązków wynikających z przepisów prawa, co wynika z art. 38 ust. 2 i 3 rozporządzenia 2016/679. W tym kontekście za słuszny uznać należy pogląd, w którym nakładanie na IOD obowiązków prowadzących do powstania konfliktu interesów, stawia pod znakiem zapytania nie tylko możliwość efektywnego wypełniania przez niego zadań, do realizacji których zobowiązuje go dyspozycja normy art. 39 rozporządzenia 2016/679, ale godzi w same fundamenty instytucji IOD, opartej w pierwszym rzędzie na niezależności jego funkcjonowania. Tym niemniej okoliczności wskazujące na niewłaściwą realizację przez Szpital obowiązków określonych w art. 38 ust. 6 rozporządzenia 2016/679, poprzez zobowiązanie IOD w okresie od dnia […] stycznia 2019 r. do dnia […] lipca 2020 r. do nadawania upoważnień personelowi w zakresie przetwarzania danych osobowych, uznać należy za udowodnione (o czym świadczy treść obowiązującej od dnia […] stycznia 2019 r. procedury […] oraz funkcjonujących od dnia […] maja 2019 r. procedur: […] oraz […], które przewidywały „uprawnienie i odpowiedzialność IOD za nadawanie upoważnień personelowi Szpitala w zakresie przetwarzania danych osobowych"). Nie pozostawia również żadnych wątpliwości, że we wzmiankowanym, szerokim przedziale czasowym IOD zmuszony był do wykonywania obowiązków powodujących konflikt interesów, a zatem nie mógł należycie sprawować swojej funkcji, co w kontekście zadań IOD przewidzianych w art. 39 rozporządzenia 2016/679 sprawia, iż wagę tego naruszenia uznać należy za znaczną." https://uodo.gov.pl/pl/353/1872 (dostęp: 2.04.2024)

C. Stanowiska wyrażane w newsletterze wydawanym przez Prezesa UODO (od kwietnia 2019 r. do listopada 2022 r.)

9. Stanowisko wyrażone w Newsletterze UODO NR 12/2020

„Jednocześnie w obowiązującym w urzędzie systemie zarządzania jakością zgodnym z normą ISO 9001:2015 przyjęto, że osobami najwyższego 4 kierownictwa są: burmistrz, jego zastępca, skarbnik i sekretarz miasta. Niemniej powzięto wątpliwości, czy na tej podstawie można wprowadzić zakładane rozwiązanie. O ich rozwianie zwrócono się więc do Prezesa UODO. W odpowiedzi organ nadzoru wskazał, że zgodnie z art. 38 ust. 3 RODO, inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub

podmiotu przetwarzającego. Służyć ma to skróceniu czasu raportowania i przepływu informacji między inspektorem a administratorem, a także wzmocnieniu niezależności inspektora, o czym mowa w motywie 97 RODO. Sposób rozumienia terminu najwyższe kierownictwo na pewno zależy od typu administratora oraz jego struktury. Niemniej należy przyjąć, że są to osoba lub osoby wchodzące w skład organu kierującego sprawami tego podmiotu. Konieczne jest bowiem zapobieganie sytuacji istnienia ogniw pośrednich, tj. kolejnych zwierzchników, między kierownictwem a inspektorem. Intencją prawodawcy jest zapobieganie sytuacji, w której pomiędzy inspektorem a najwyższym kierownictwem (dyrektorem, prezesem itp.) istniałyby ogniwa pośredniczące (kolejni zwierzchnicy, np. kierownik działu), ponieważ sytuacja taka może prowadzić do ograniczenia efektywności działań inspektora ochrony danych. W przypadku gdyby inspektor podlegał kierownikowi, a ten miałby nad sobą kolejnego zwierzchnika – dyrektora, który z kolei podlegałby prezesowi, to możliwość bezpośredniego wskazania najwyższemu kierownictwu potrzeb i problemów dotyczących ochrony danych byłaby ograniczona (mogłoby się okazać np. że kierownik nie przekaże informacji, dalej uznając, że nie są one wystarczająco istotne) (por. komentarz do art. 38 RODO w: Fajgielski Paweł, Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, WKP 2018). Tymczasem zgodnie z art. 11a ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, organami gminy są rada gminy oraz wójt, burmistrz lub prezydent miasta. Oznacza to, że w przypadku urzędu miasta najwyższym kierownictwem, w rozumieniu przepisów o ochronie danych osobowych, jest burmistrz. Sekretarz miasta podlega w wykonywaniu swoich obowiązków burmistrzowi, a więc byłby dodatkowym ogniwem pośredniczącym między administratorem a inspektorem

10. Stanowisko wyrażone w Newsletterze UODO NR 10/2022

„Za przyjęciem takiej interpretacji art. 38 ust. 3 zdanie drugie RODO opowiada się również organ nadzorczy. W jego opinii art. 38 ust. 3 zdanie drugie RODO nie stoi na przeszkodzie przepisowi prawa krajowego, na mocy którego inspektor ochrony danych uzyska dalej idącą ochronę prawną przed odwołaniem lub karaniem. Art. 38 ust. 3 RODO jest bowiem ogólnym wskazaniem zasady, jaką powinny kierować się państwa ze względu na bezpośredniość stosowania unijnego rozporządzenia. Ustawodawca polski, wprowadzając do porządku prawnego nowe regulacje prawne na podstawie RODO, zwłaszcza ustawę z dnia 10 maja 2018 r. o ochronie danych, nie uregulował w żaden szczególny sposób ochrony pełnienia funkcji IOD. Dlatego regulacje szczegółowe dotyczące ochrony stabilności pełnienia tej funkcji powinny zostać doprecyzowane we właściwych przepisach obejmujących zarówno przypadki stosunku pracy, jak i umowy o świadczenie usług. TSUE w powołanym wyroku ocenił, że art. 38 ust. 3 zdanie drugie RODO ma zastosowanie zarówno do IOD będącego członkiem personelu administratora danych lub podmiotu przetwarzającego, jak i do osoby wykonującej te zadania na podstawie umowy o świadczenie usług, zgodnie z art. 37 ust. 6 RODO (pkt 23 wyroku). Pozycja inspektora ochrony danych w obu przypadkach powinna zatem zostać wzmocniona.”

11. Stanowisko wyrażone w Newsletterze UODO NR 8-9/2022

„ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (wdrażająca do polskiego porządku prawnego tzw. dyrektywę policyjną, czyli dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję

ramową Rady 209/977/WSiSW) wymaga zmian w zakresie przepisów dotyczących inspektora ochrony danych. Błędne przypisanie zadań W ocenie UODO zmiany wymagają art. 37 ust. 3 i art. 38 ust. 6 powołanej ustawy z dnia 14 grudnia 2018 r., gdyż są one sprzeczne z przepisami tzw. dyrektywy policyjnej. Z przepisów tych wynika, że zarówno przeprowadzenie oceny skutków dla ochrony danych, jak i uprzednich konsultacji administrator może powierzyć inspektorowi ochrony danych. Tymczasem przeprowadzenie oceny skutków dla ochrony danych i wystąpienie z wnioskiem o uprzednie konsultacje do organu nadzorczego to zadania administratora i to właśnie jemu są one przypisane w dyrektywie. Ich realizacja przez IOD prowadziłaby zaś do powstania konfliktu interesów. Błędna i wymagająca zmiany jest również redakcja art. 38 ust. 6. Artykuł ten stanowi, że realizację obowiązków, o których mowa w ust. 1— 4 tego artykułu, administrator lub podmiot przetwarzający może powierzyć inspektorowi ochrony danych. Tymczasem ust. 2 i 4 tego przepisu odnoszą się do zadań Prezesa UODO, wobec tego przypisanie ich IOD oznacza błędne sformułowanie przepisu”

12. Stanowisko wyrażone w Newsletterze UODO NR 2/2021

„Kształtując zatem zakres obowiązków IOD warto pamiętać, że inspektor nie powinien realizować zadań, które mogą stać się następnie przedmiotem dokonywania przez niego czynności monitorowania ani podejmować decyzji w zakresie celów i środków dotyczących przetwarzania i zabezpieczania danych.”

13. Stanowisko wyrażone w Newsletterze UODO NR 1/2021

„Niedopuszczalne jest wyznaczenie do pełnienia funkcji inspektora ochrony danych (IOD) osoby kierującej (zarządzającej) podmiotem posiadającym status administratora, takiej jak np. członek zarządu stowarzyszenia lub spółki, dyrektor szkoły, wójt. W opinii organu ds. ochrony danych osobowych, do takich osób należy również przewodniczący zakładowej organizacji związkowej, właśnie ze względu na swoją rolę polegającą na zarządzaniu/kierowaniu działalnością tej organizacji.”

D. Stanowiska wyrażane w biuletynie wydawanym przez Prezesa UODO (od grudnia 2022 r. do lutego 2024 r.)

14. Stanowisko wyrażone w Biuletynie UODO NR 2/04/23

„W czasie prowadzonych postępowań stwierdzono liczne nieprawidłowości dotyczące powołania i funkcjonowania inspektorów ochrony danych, które dotyczą takich kwestii, jak np.: niewłaściwe włączanie IOD w sprawy dotyczące ochrony danych osobowych, niepodejmowanie działań mających na celu zapewnienie inspektorowi ochrony danych zasobów niezbędnych do utrzymania jego wiedzy fachowej, brak procedur zapewniających niezależność inspektora ochrony danych, w szczególności dotyczących zakazu otrzymywania instrukcji, wydawania poleceń, jak również zapewnienia, że w ramach wykonywania zadań inspektora ochrony danych nie będzie on odwoływany ani karany. Wiele z naszych zastrzeżeń związanych też było z nałożeniem na inspektorów ochrony danych zadań, które należą do obowiązków administratorów, jak np. prowadzenie rejestru czynności przetwarzania, rejestru naruszeń ochrony danych osobowych czy tworzenia wewnętrznych polityk. Inspektor nie może bowiem być obciążony działaniami, które ma oceniać pod kątem ich zgodności z przepisami prawa i regulacjami wewnętrznymi administratora.”

15. Stanowisko wyrażone w Biuletynie UODO NR 3/05/23

„Komplementariusz, gdy jest jednocześnie wspólnikiem spółki komandytowej i osobą reprezentującą tę spółkę zgodnie z umową spółki komandytowej, czyli prowadzi sprawy spółki

(kieruje jej działalnością) i decyduje o celach i sposobach przetwarzania danych osobowych, nie może równolegle zajmować stanowiska inspektora ochrony danych”

16. Stanowisko wyrażone w Biuletynie UODO NR 01/01/2024

„Rola IOD jako punktu kontaktowego dla osób, których dane dotyczą, jest mocno powiązana z obowiązkami administratora i ma przyczyniać się do skuteczniejszego ich wykonywania. Rolą IOD jest bowiem budowanie świadomości administratora w zakresie praw tych osób, a następnie monitorowanie skuteczności przyjętych w tym zakresie procedur i rozwiązań, a gdy to konieczne – proponowanie ich modyfikacji. Zgodnie z powołanym powyżej art. 38 ust. 4 RODO osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Stosowanie tego przepisu nie powinno prowadzić do wyręczania administratora przez IOD w jego obowiązkach, ponieważ IOD nie mógłby przez to realizować własnych zadań, tj. w sposób niezależny monitorować i doradzać administratorowi w zakresie tych obowiązków. Nieprzestrzeganie rozróżnienia tych dwóch ról mogłoby doprowadzić do powstania konfliktu interesów, którego występowania zakazuje w odniesieniu do IOD art. 38 ust. 6 RODO. Dlatego rolę punktu kontaktowego należy rozumieć tu raczej jako wsparcie dla osób, których dane dotyczą w sytuacjach, w których osoby zgłosiłyby zastrzeżenia, trudności czy wątpliwości co do wykonywania praw przysługujących im na mocy RODO. IOD nie powinien być pełnomocnikiem administratora Jednocześnie organ nadzorczy zaznaczył, że IOD nie powinien być pełnomocnikiem administratora. Zadaniem pełnomocnika jest ochrona interesów mocodawcy, działanie według instrukcji i sugestii mocodawcy, co stoi w sprzeczności z niezależnością inspektora ochrony danych, zagwarantowaną w RODO, w tym w art. 38 ust. 3 RODO. Zgodnie z tym przepisem, administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Pełnienie roli pełnomocnika przez IOD w sprawach z zakresu ochrony danych osobowych u administratora, u którego IOD pełni swoją funkcję, stoi ponadto w kolizji z nakazem nienakładania.”

E. Stanowisko zawarte w sprawozdaniu krajowym Prezesa UODO w ramach badania CEF

„W wyniku działań UODO polegających na weryfikacji przestrzegania przepisów dotyczących IOD w kilku organizacjach zidentyfikowany został problem nakładania przez administratora na IOD zadania dotyczącego prowadzenia rejestru czynności przetwarzania, co powoduje konflikt interesów, o którym mowa w art 38 ust. 6 RODO. IOD nie może bowiem podejmować działań lub decyzji, które następnie muszą podlegać jego ocenie zgodnie z art. 39 ust. 1 lit. b RODO. Z brzmienia art. 30 ust. 1 RODO wynika, że prowadzenie rejestru czynności przetwarzania należy do obowiązków administratora. W ocenie UODO obecne brzmienie Wytycznych dotyczących inspektorów ochrony danych WP 243 rew.01 dopuszczające możliwość wykonywania przez IOD zadania administratora, jakim jest prowadzenie rejestru czynności przetwarzania, wymaga dostosowania do aktualnego stanu prawnego. Realizowanie tego zadania przez IOD prowadzi do powstania konfliktu interesów, którego występowania zakazuje w odniesieniu do inspektorów art. 38 ust. 6 RODO. (…) Rzeczywiście katalog zadań inspektora ochrony danych nie jest zamknięty, niemniej w przypadku nakładania na IOD innych zadań należy zawsze uwzględnić art. 38 ust. 6 RODO, tj., że zadania nakładane przez administratora na IOD nie mogą powodować konfliktu interesów. Warto nadmienić, że takie rekomendacje co do dopuszczalności prowadzenia rejestru czynności przetwarzania przez IOD polski organ nadzorczy opublikował na swojej stronie internetowej (https://archiwum.uodo.gov.pl/pl/225/659). Wyjaśnił tam, że zgodnie z art. 30 ust. 1 i 2 RODO, do administratora należy obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada, a do podmiotu przetwarzającego - prowadzenie rejestru

kategorii czynności przetwarzania dokonywanych w imieniu administratora. To te podmioty są odpowiedzialne za efektywne wykonanie tego obowiązku i pozostawanie w gotowości do wykazania tego na żądanie organów ochrony danych. Natomiast inspektor ochrony danych jako fachowiec może jedynie wspomagać administratora w tworzeniu i prowadzeniu rejestrów na przykład poprzez doradzanie mu w kwestiach związanych z wykonaniem tego obowiązku. Kolejnym zidentyfikowanym problemem była kwestia udzielenia inspektorowi ochrony danych pełnomocnictwa do występowania w imieniu administratora (reprezentowania administratora) przed organem nadzorczym i sądem w sprawach z zakresu ochrony danych osobowych. Wprawdzie polskie procedury postępowania zarówno przed sądem, jak i organem nadzorczym nie przewidują wprost wyłączenia inspektora ochrony danych z kręgu osób mogących być pełnomocnikami w sprawach z zakresu ochrony danych, ale udzielenie takiego pełnomocnictwa jest sprzeczne z zakazem nakładania na IOD zadań powodujących konflikt interesów (art. 38 ust. 6 RODO) oraz zakazem udzielania inspektorowi instrukcji co do wykonywania zadań (art. 38 ust. 3 RODO). Zadaniem pełnomocnika jest ochrona interesów mocodawcy, działanie według jego instrukcji i sugestii, co stoi w sprzeczności z zagwarantowaną w RODO niezależnością inspektora ochrony danych. Natomiast głównym celem IOD nie jest działanie wyłącznie w interesie administratora, na co wskazują zarówno zakres zadań IOD, jak i gwarancje jego niezależności. Podstawowym zadaniem IOD jest m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych przez administratora i doradzanie mu w tym zakresie. Pełnienie roli pełnomocnika przez IOD w sprawach z zakresu ochrony danych osobowych stoi zatem w kolizji przede wszystkim z zakazem nakładania na IOD zadań powodujących konflikt interesów. IOD, działając jako pełnomocnik administratora w sprawach ochrony danych osobowych przed organem nadzorczym lub sądem, składa w imieniu mocodawcy wyjaśnienia dotyczące przetwarzania danych osobowych przez administratora. Działając zgodnie z wolą i interesem mocodawcy, w wyjaśnieniach tych mógłby być zmuszony do pomijania własnych spostrzeżeń i rekomendacji, które wypracował jako IOD. Polski organ nadzorczy w odpowiedziach na pytania inspektorów dotyczących tego zagadnienia, oprócz powyższych argumentów wskazywał, że IOD - z uwagi na swoją rolę fachowego doradcy i podmiotu monitorującego w sposób niezależny przestrzeganie przepisów o ochronie danych osobowych - powinien ze swej strony odpowiednio wcześnie identyfikować i sygnalizować administratorowi ryzyko wystąpienia takiego konfliktu. Dzięki temu możliwe jest odpowiednio wczesne zapobieganie mu. W takim przypadku inspektor ochrony danych powinien powstrzymać się od dokonywania czynności w imieniu administratora lub wypowiedzieć udzielone mu pełnomocnictwo. Innym ważnym problemem, na który zwrócił uwagę polski organ nadzorczy, jest nieprawidłowa praktyka polegająca na zawieraniu umowy powierzenia przez administratora z IOD, który nie jest jego pracownikiem. UODO odnosił się do tego problemu, publikując na swojej stronie internetowej odpowiedzi na pytania inspektorów dotyczące tego problemu (https://archiwum.uodo.gov.pl/pl/223/2050, https://archiwum.uodo.gov.pl/pl/223/2092). Wskazywał w nich, że zawieranie umowy powierzenia przez administratora z IOD stoi w kolizji z zakazem udzielania IOD instrukcji co do wykonywania zadań i niedopuszczania do zaistnienia konfliktu interesów. Zgodnie z RODO podmiot przetwarzający jest zobowiązany do stosowania się do instrukcji przekazanych przez administratora. Natomiast w odniesieniu do inspektora ochrony danych administrator i podmiot przetwarzający mają m.in. obowiązek zapewnić, aby inspektor nie otrzymywał instrukcji dotyczących wykonywania swoich zadań (art. 38 ust. 3 RODO). Ponadto możliwość wykonywania przez osobę, z którą zawierana jest umowa o świadczenie usług, zadań innych niż określone w RODO ograniczona jest zakazem występowania w tym zakresie konfliktu interesów (art. 38 ust. 6 RODO). Sednem ww. stanowiska jest, że występowanie inspektora ochrony danych w charakterze podmiotu przetwarzającego, który ma realizować zadania związane z przetwarzaniem danych w imieniu i na rzecz administratora oraz jest zobowiązany do stosowania się ściśle do instrukcji przekazanych mu w tym zakresie przez administratora,

narusza niezależność IOD. Natomiast w relacji administrator - podmiot przetwarzający nie ma przestrzeni na niezależne działanie podmiotu przetwarzającego, w jakimkolwiek stopniu niezgodne z instrukcjami administratora. Z tego powodu IOD nie może występować w roli podmiotu przetwarzającego (być stroną umowy powierzenia) i działać na polecenie administratora, bo stoi to w sprzeczności z niezależnością inspektora gwarantowaną przez przepisy RODO. Niezależność ta jest niezbędna, aby inspektor mógł w sposób prawidłowy realizować swoje zadania wymienione w art. 39 ust. 1 RODO.”